User's Guide

FlexWATCH^{TM} 3110

(Version. 3.0_Rev0)

Seyeon Technology Co., Ltd
www.flexwatch.com
www.intplus.es

Table of Contents

Overview of FlexWATCH^{TM} Server 10

1 Packing List 10

2 What is FlexWATCH^{TM}? 11

2.1 Key Function of FlexWATCH^{TM} 11
2.2 Product Specification 12
2.3 Basic Network Connection Diagram 13
2.4 Application 15

3 Hardware Description 17

3.1 Caution and observance 17
3.2 Hardware Description 17

IP assignment 19

1 Key Words for Network 19

2 Check Points before IP assignment 21

2.1 IP address 21
2.2 LAN cable or Cross-Over Cable 23
2.3 PC Environment 25

3 Factory Default 25

4 IP Assignment 25

4.1 Through Installation Wizard Program 25
4.2 IP Assignment through Hyper Terminal mode 28

Live view & Camera Configuration 33

1 Live View 33

1.1 ActiveX based simple view 33
1.2 Java Applet based live view 34
1.3 Live view page guide 34

2 FW-Voyager based view and recording 36

3 Camera configuration 36

3.1 Camera value string configuration... 36
3.2 Camera configuration... 38
3.3 Video Motion Detection 40

System Configuration 43

1 System Information.. 43

2 Date & Time 43

2.1 Date & Time in the server clock 43
2.2 Date & Time using NTP server 44

3 Admin Password Setup 44

4 Access Control and User registration 44

4.1 Full Access 45
4.2 Limited Access and User registration 45

5 Frame rate control 47

6 Tx Module Registration(NVCP)... 48

Network Configuration 51

1 Network configuration... 51

1.1 Static IP 51
1.2 DHCP Client... 51

2 PPPoE Configuration 53

3 Network port configuration 54

3.1 HTTP port configuration 54
3.2 NVCP –Tx Port 54
3.3 VDCP Port configuration 54

4 WAN Configuration and Application 55

4.1 External Modem connection 55
4.2 Application with Dial-in/out feature 55
4.3 Dial Out configuration 56
4.4 Dial-in Configuration 58

5 Service Path 59

6 AOIP Setup 60

6.1 How to use AOIP service 60
6.2 AOIP configuration 61

7 Network Status 62

External Device connection & configuration 63

1 Serial Ports Configuration Guide 63

1.1 Hardware Description 63

2 Installation & Configuration of External Device 66

2.1 Console(Hyper Terminal cable connection) 66
2.2 Serial Input device 67
2.3 Serial output device 68
2.4 PTZ device connection and configuration 70
2.5 Voice Kit Connection and configuration 73

3 Alarm input device connection 75

4 Alarm Output(Relay output) device connection 75

4.1 Alarm output device connection 76
4.2 Manual control of Alarm output device 76
4.3 Automatic Control of Alarm Output device 77

Advanced Service configuration 79

1 Buffering Service 79

1.1 System and Pre Alarm Buffer memory 80
1.2 Buffer calculator 82

2 Service Condition 84

2.1 Condition Setup 85
2.2 Criteria Setup 86

3 e-mail configuration 88

3.1 e-mail function configuration 88
3.2 e-Mail condition set up 90

4 FTP Configuration 90

4.1 Directory option 90
4.2 FTP service configuration 93

5 Alarm Buffering Service 95

5.1 Alarm Buffering Service Configuration 95
5.2 Playback of Pre/post alarm Image 96

6 Sensor Notification service 97

Utilities 99

1 Save Configuration 99

2 Reboot 99

3 Factory Default 99

4 System Update 100

4.1 Description of files system 100
4.2 Update Procedure 102

Notice

- The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Seyeon Tech assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein.
- Seyeon Tech reserves the right to make changes in the product design without reservation and without notification to its users.

Copyright

Copyright© 1999-2004 Seyeon Tech Co., Ltd. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of Seyeon Tech Co., Ltd.

Copyright © 1999-2005 Seyeon Tech Co., Ltd.

810-12 Yeok Sam-dong,
Kang Nam-gu, SEOUL,
135-081,KOREA
TEL : 82 2 3017 0855
FAX : 82 2 3017 0843
URL : http://www.seyeon.co.kr
http://www.flexwatch.com

Warning

To prevent risk of electric shock, **Do not** remove system-case. No user serviceable parts inside. Any repair or modification for the product will be allowed to qualified service personal only.
Do not expose this appliance to water or moisture.
Do not install this product in Hazardous areas where highly combustible or explosive products are stored or used.

Important Information

- Before installation, please read and observe all instructions and warnings contained in this manual. Retain this manual with the original receipt for future reference and warranty.

- If any items are missing from the package when you open the box, please DO NOT install or OPERATRE FlexWATCH™ server. Contact the local Dealer or Distributor.

- Please record following information **for technical support and the track record** in case of any theft or loss. Serial Number can be found underside of FlexWATCH™ server

Product Model : ____________________________
Purchase Date : ____________________________
Serial Number : ____________________________

Overview of FlexWATCH™ Server

1 Packing List

Please check and make sure following items are included in your package without any missing items.

If there are any missing items, please refer to your local distributor.

A. FlexWATCH™ 3110……………………………………………………………………….1unit

FlexWATCH™ 3110

B. RS-232 Serial cable……………………………………………………………………1unit

(Cross cable DB9 Female)

C. Power Adapter………………………………………………………………………….1unit

(Power Cable, SMPS DC 12V Adapter)

D. User's Manual CD……………………………………………………………… 1unit

2 What is FlexWATCH™?

The FlexWATCH™ server is the Network Video Server, which transmits digital images captured by Analog CCD camera over the Internet. So users can view real-time live images over the Internet at anytime and anywhere using the standard web browser such as MS Internet Explorer or Netscape Communicator. There is no need other specific software to view real-time live images over the Internet. The FlexWATCH™ server is state-of-the art device and leads new generation of monitoring and security solution.

2.1 Key Function of FlexWATCH™

Self contained stable system

Built-in Web server, Real time operation system and hardware video compression engines are included. No **PC required to transmits real time video** over the TCP/IP network.

High performance of video transmission

30fps (NTSC)/25FPS(PAL) per each channel and 120fps (NTSC)/100fps(PAL) **for 4 cameras at 5kbps image size.**

Channel based user authentication

Channel based **multi user level protection** for camera control, PTZ control, Alarm output and Audio control.

2400 frames Pre/Post video alarm buffer

2400 frames pre/post alarm buffer **to store event triggered video in the internal memory.**

Built-in Motion detection and time stamp

Built-in motion detection per each camera with up to 144 block of motion area to filter out unnecessary motion detection area. Optional time stamp on the video.

2.2 Product Specification

Hardware

- 32bit Embedded CPU
- Flash 4Mbytes /SDRAM: 32Mbytes
- Hardware Motion JPEG engine
- Linux version 2.4.xx operating system

System Requirements

- OS : Windows 95/98/2000/XP/NT/ ME, Linux, Mac, Unix, Linux Operation system.
- Browser : MS Internet explorer(5.x or above) Netscape(6.x or above)
- PC H/W Pentium III 500M or above
- RAM: 64 MB and above

Network Protocols

- HTTP, TCP/IP, FTP, Telnet, RARP, PPP, PAP, CHAP, DHCP, SMTP client(e- mail), NTP, Java

Video

- NTSC: 704x480,704x240,352x240,176x112
- PAL : 704x576,704x288,352x288,176x144
- NTSC/PAL video auto sensing
- Frame Rate : **30fps** 352X240 / 352x288
  * based on Pentium4 2.0G and 100M dedicated network
- Image quality: 6 levels

Auxiliary Video-in & output

- 1 video inputs & 1 loop through outputs

LAN Interface

- 10/100BaseT Ethernet auto negotiation

Alarm I/O interface

- 1 Opto-coupled inputs or 1digital inputs
- 1 Relay output

Serial Interface

- Two serial ports for console, modem (PSTN & GSM), serial input/output device, PTZ or voice kit
- Each port can be configured as RS-232, RS-485 or RS-422(max 115kbit/s)

Security features

- Channel based multi user level protection for camera access, PTZ, Alarm I/O, Voice
- IP address Filtering / Image Encryption

Advanced Service

- Up to 5M Pre/Post alarm buffer memory
- Built-in Motion detections (Up to 144 blocks)
- e-mail, FTP, alarm Buffer by event or schedule
- IP notification, Alarm Notification to e-mail, CGI path by event or schedule

PTZ & UART Control

- PTZ and UART device control through serial interface
- Up to 29 PTZ protocols from Panasonic Dome, Pelco "P" & "D" protocol, Sony EVI- D30, Kalateland AD Delta dome, Vicon Surveyor,CannonVC-C4 and etc. Refer to user guide for more vendors
- X10 device control

Others

- Video loss detection
- Up to 100 concurrent user access
- Dial in/out via PSTN or GSM modem
- Time stamp on Video
- Transmit Serial input data transfer with Video
- **IP notification by e-mail**

Developer support

- Provides HTTP CGI API
- ActiveX control development kit

Management

- Configurable by serial, web or telnet
- Remote system update via telnet, FTP or web browser.

Dimension

- Size: 122mm(W) x 84mm(D) x 35mm (H)
- Weight : 0.5kg without power supply

PWR Supply

- DC 12 Volt, 1.5Am, SMPS

Operating temp

- 40° ~ 125°F (5° ~ 50°C)

Approval

- FCC : Class A/ CE : Class A

Accessories

- Console cable for system set up/ LAN cable
- CD for User Guide, Installation wizard & Technical note
- Quick Installation guide

Miscellaneous

- Voice kit(FW-V10s) support
- Freely downloadable NDVR Software
- AVI conversion tool support by FW-voyager
- Work with FW-Manager NDVR S/W

· Dynamic IP support through AOIP

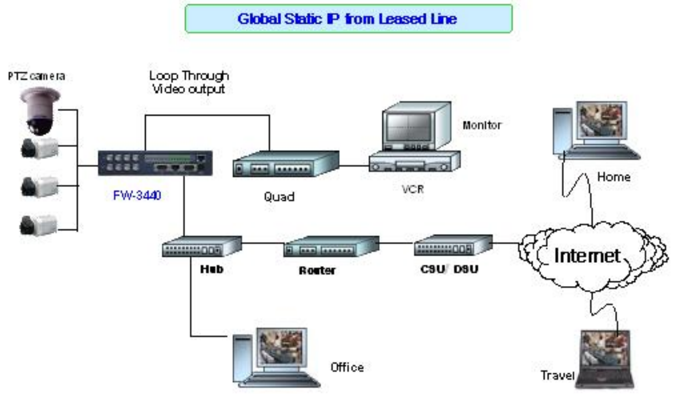
2.3 Basic Network Connection Diagram

FlexWATCH^{TM} server provides flexible connectivity with any type of networks available around you such as Leased line, Cable modem, xDSL line and PSTN (POT) line. Thus, it can be installed either in LAN or WAN environment as long as there is network available. But its configuration is subject to change depending on its environment. Following is basic network diagram for using FlexWATCH^{TM} server.

Thus, you are required to consult with your network administrator or network consultant for more information. Also you are recommended to refer to Network configuration guide in the CD manual for more details.

2.3.1 Leased Line connection

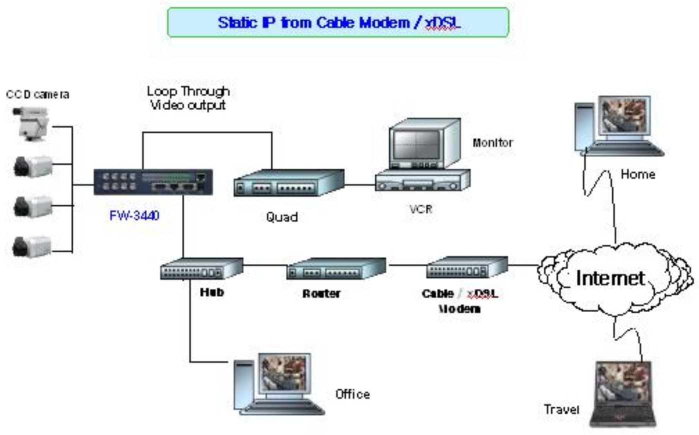
Simply get a Static IP address from Network Administrator and assign IP address to FlexWATCH^{TM} server and view from the Internet.


Global Static IP from Leased Line
PTZ camera
Loop Through
Video output
Monitor
Home
FW-3440
Quad
VCR
Hub
Router
CSU/ DSU
Internet
Office
Travel

2.3.2 Static IP address from Cable modem or xDSL line

Simply get a Static IP address from Network Administrator or ISP and assign IP address to FlexWATCH^{TM} server and view from the Internet

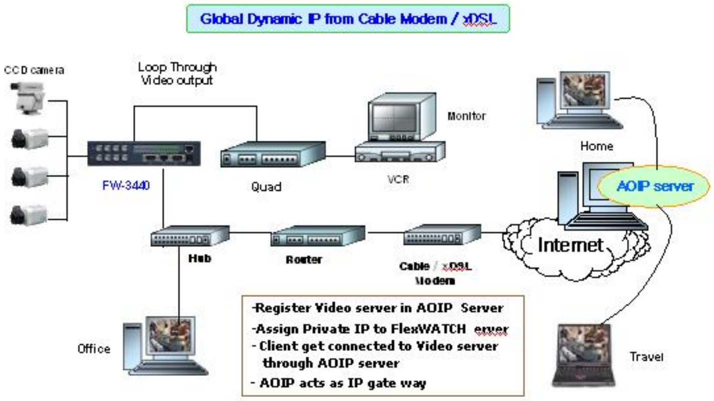
Static IP from Cable Modem / xDSL


CCD camera
Loop Through
Video output
Monitor
Home
FW-3440
Quad
VCR
Internet
Hub
Router
Cable / xDSL
Modem
Office
Travel

2.3.3 Dynamic IP address from Cable or xDSL line

FlexWATCH^{TM} server can be installed on even Dynamic IP network. But it needs to be registered in AOIP server which is an IP gateway running by Flexwatch.com or your local Distributor. For more details, please refer to Technical guide book in the CD manual.

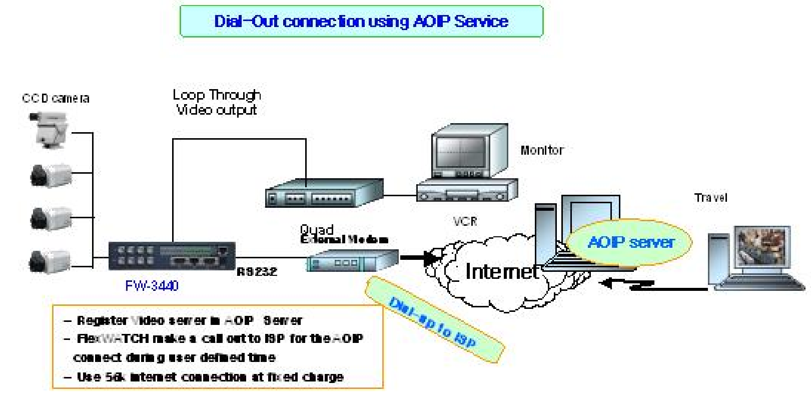
Global Dynamic IP from Cable Modem / xDSL


CCD camera
Loop Through
Video output
Monitor
Home
AOIP server
FW-3440
Quad
VCR
Internet
Hub
Router
Cable / xDSL
Modem
Office
Travel

-Register Video server in AOIP Server
-Assign Private IP to FlexWATCH erver
- Client get connected to Video server through AOIP server
- AOIP acts as IP gate way

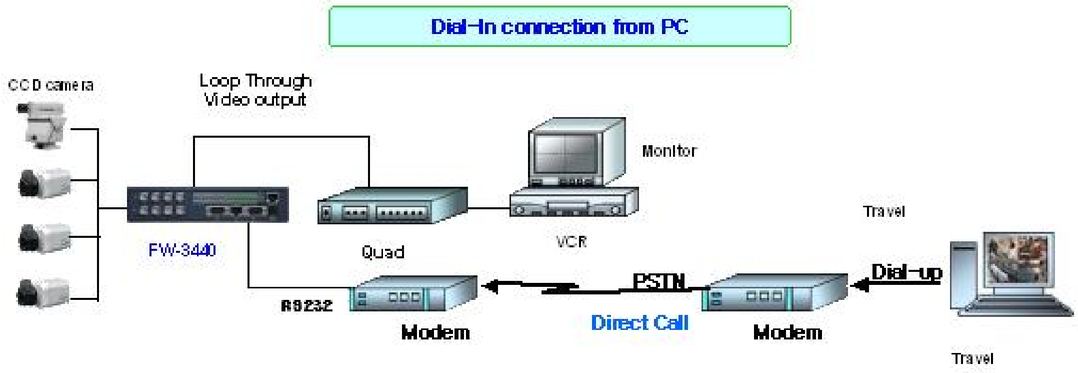
2.3.4 Dial-up to AOIP server

Using Dial-up function of FlexWATCH^{TM} server and AOIP service, you can set the FlexWATCH^{TM} server to make a call to ISP and get it connected AOIP server. Once FlexWATCH^{TM} server is registered in AOIP server, you can connect FlexWATCH^{TM} server through AOIP server. Using this connection, you do not need to make multiple call or international call to FlexWATCH^{TM} server, since FlexWATCH^{TM} server will be connected by your local Phone line based Internet connection.


Dial-Out connection using AOIP Service
CCD camera
Loop Through Video output
Monitor
Quad
VCR
External Modem
Travel
AOIP server
Internet
RS232
FW-3440
Dial-up to ISP
– Register Video server in AOIP Server
– FlexWATCH make a call out to ISP for the AOIP connect during user defined time
– Use 56k internet connection at fixed charge

2.3.5 Dial-in to FlexWATCH^{TM} server through PSTN line

You can make a call to FlexWATCH^{TM} server from anywhere and at anytime. But if you are concerned about call charge, we are recommending using above connection.


Dial-In connection from PC
CCD camera
Loop Through Video output
Monitor
FW-3440
Quad
VCR
Travel
RS232
Modem
PSTN
Direct Call
Modem
Dial-up
Travel

2.4 Application

Unlimited application for remote monitoring and surveillance solution can be built up using FlexWATCH^{TM} server and its supporting peripheral Hardware and software such as FW-5000 or FW-5440 Network video recorder

server and ***FW-Manager*** DVR software.

Following could be simple application area where FlexWATCH^{TM} server can be applied.

A. Building live home pager for advertising.

B. ITS (Intelligent Traffic System) for real time monitoring

C. IBS (Intelligent Building System) using FlexWATCH^{TM} Manager

D. Internet broadcasting

E. School, Kindergarten, Nursery, Franchised Restaurant & convenient store.

F. Facility monitoring

3 Hardware Description

- This chapter contains list of items to be prepared for the installation of FlexWATCH^{TM} server.
- Please carefully read this chapter before the installation.
- Please prepare all the necessary items before start installation to prevent any possible malfunction or any other hazard can be happened during the installation.

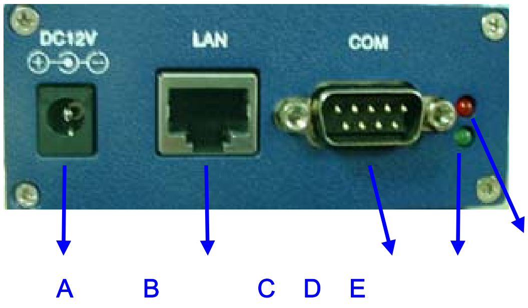
3.1 Caution and observance

- Keep the device in the clean and dried area where air ventilation is guaranteed. The device is not waterproof. The waterproof device or similar device must protect from any possible hazard by water or heavy moisture etc.
- Regulated power supply is prerequisite for stable and optimal operation of the device. Use only power supply (SMPS 12V 1.5Am) supplied with FlexWATCH^{TM} server. Manufacturer shall not liable for any hazard or shock caused by use of any other power supply.
- To prevent risk of electric shock, do not remove system-case. No user serviceable parts inside. Any repair or modification for the product will be allowed to qualified service personal only
- Use the cable supplied with FlexWATCH^{TM} server. If you need to connect FlexWATCH^{TM} server to the other device (External Modem, PTZ device), power on the devices before connect to the FlexWATCH^{TM} server.

3.2 Hardware Description

3.2.1 FW-3110 Hardware Description

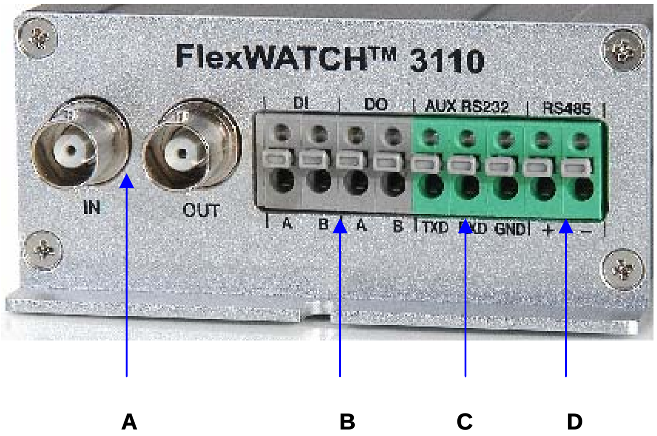
Front Panel View



Menu Description

A	**DC12V**	DC 12V power
B	**LAN**	LAN Port for 10/100M Base T Auto sensing
C	**COM**	RS-232 port for serial input device, Voice kit, PTZ. **Console for Hyper Terminal must be connected to this port only**.
D	**LAN LED**	Blinking only when LAN is connected to the network Green-light on when LAN connection is OK
E	**PWR LED**	Indicate power on/off Always red-light on when turned on

Rear Panel View



A	**BNC IN/OUT**	4Video input and 4 loop through video output
B	**General I/O**	1 Opto-coupled input and 1 output
C	**RS-232**	RS-232 Port to connect Serial input device, Voice kit, PTZ device or Modem.
F	**RS-485**	To connect RS-485 based PTZ device. For more information, refer to External device configuration menu.

IP assignment

1 Key Words for Network

LAN (Local Area Network) : Under the LAN network, any network device in the same LAN network can be accessed by any other network device. But LAN network can not be accessed from the Internet (WAN).

Most of case, LAN is built after Router which is connected to WAN network so that Network device in the local area network can access to the Internet through Router. Most of case, LAN networked device can not be accessed from the Internet (WAN), unless it is not configured to be accessed from the Internet through NAT function of router.

WAN (Wide Area Network) : WAN enables all network device can be accessed by each other over the Internet. It included Leased Line, Cable modem, xDSL, ISDN and Telephone line etc.

IP address : IP address is abbreviation of Internet Protocol address which allows all network devices can communicate other over the network using Internet protocol. Each network device has its own unit IP address whether or not it is in the LAN or WAN network. Therefore network devices can be accessed by other network device from either LAN or WAN (Internet).

For example, www.yahoo.com is a web server which has its own IP address so that any body can has access to Yahoo web site. Like most of public web site has its own IP address. Although IP address can not be seen by the client, domain name (www.yahoo.com) is automatically converted into IP address by DNS server.

Static IP address : A static IP address is an IP address permanently assigned to computer or network devices in a TCP/IP network. Static IP address is usually assigned to network devices which are consistently accessed by any users. For instances, www.yahoo.com has global static IP address. Thus, any body can access to the site. If you want to view live video stream from FlexWATCH^{TM} server over the Internet, you need to assign Global Static IP address.

Depending the network Public Static IP(WAN) or Private Static IP can be assigned to network device.

Dynamic IP address : A dynamic IP address is an IP address that is automatically assigned to a client station (computer, network equipment, etc.) in a TCP/IP network. Dynamic IP address is typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as router. A dynamic IP address may change every time your computer connects to the network

DHCP (Dynamic Host Configuration Protocol) : DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DCHP eliminates troublesome job to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as routers. Most of Cable Modem for Internet access uses DHCP Public IP address and Private IP address : Public IP address is an IP address which can be identified uniquely in Internet world. All IP addresses excluding private IP addresses are public IP addresses. Private IP addresses range from 10.0.0.0 until 10.255.255.255, and from 192.168.0.0 to 192.168.255.255. Generally speaking, private IP addresses are used in local area network which are hidden from the Internet world. Also, when public IP addresses not enough, private IP addresses are used while sharing global IP addresses

Router : Router is a network hardware which routes either Private or Public IP address to Public network so that network device between private IP network and Public IP network can communicate over the network. Router has NAT (Network Address Translation) function and through this function Public IP address will be mapped into private IP network so that Network device in the private IP address can be added from Internet.

Hub : Hub is a hardware which relay transmission between Router and Network device. There are two types of Hub. One is Dummy hub and the other one is Switching hub. Note that Hub will be used in the local network only.

NAT (Network Address Translation) : Network Address Translation (NAT) translates multiple IP addressed on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private

LAN is never transmitted on the Internet.

AOIP (Always On Internet Protocol) Server: AOIP™ server (Always On IP) is run by Seyeon Technology or its business partner and is a gateway for remote users to access FlexWATCH™ servers which is connected dynamic IP address over DSL,Cable modem and PSTN network over the Internet. FlexWATCH™ Network Video Server and Camera Server family is fully supported by AOIP server and any type of IP address(Global Dynamic IP or Private IP) can be assigned to FlexWATCHTM server and user can access FlexWATCH™ system from the Internet at anytime and anywhere through AOIP server.

2 Check Points before IP assignment

Following are list of item to be checked before you start configuration of FlexWATCHTM server.

2.1 IP address

You need to have Static IP address and other information such as Default Gateway and Network Mask which are to be assigned to FlexWATCH^{TM} server. Please consult with your network administrator, if FlexWATCH^{TM} server is to be installed in your corporate network, or consult with ISP if you want to install it in your home or shop for which DSL or Cable modem Internet service is available.

Following could be a simple way of finding IP address information of your PC and with that information you can set up IP address to FlexWATCH^{TM} server in the private IP network without consulting to your ISP.

- Open DOS Command window as following procedure.

Program> Accessories > DOS Prompt

- Enter ***' ipconfig'*** command. Following information will come up

2.1.1 Static IP address enabled PC (DHCP Disabled PC)

You can easily check whether Static IP address is assigned to your PC. If you are in the Static IP network, it is simpler to assign IP address to FlexWATCH^{TM} server than DHCP network.

\

```
C:\> ipconfig
Windows 2000/XP IP Configuration
Ethernet adapter Local area connection :

    Connection-specific DNS Suffix  . :
    IP Address. . . . . . . . . . . : 192.168.0.158
    Subnet Mask . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . : 192.168.0.1
C:\>
```

With above info, you can get information about your network from your PC and see which IP class of IP address should be assigned to FlexWATCH™ server.

Note that the same class, but different IP address appeared in your PC must be used for FlexWATCH™ server to assign an IP address from your PC keeping Subnet mask & default gateway as same that of your PC.

For example, 192.168.0.155 or other available IP address except 192.168.0.158 can be assigned to FlexWATCH™ server, since it is the same class of your IP address and can be communicated in your local network.
If you want to check out whether 192.168.0.155 is available. Please try ping command in the DOS window. If there is any response, it means 192.168.0.155 is assigned to other network device. Thus, you need to randomly select other IP address and try ping test or consult with your network administrator

```
C:\> ping 192.168.0.155
Pinging 192.168.0.155 with 32 bytes of data:
```

```
Reply from 192.168.0.155: bytes=32 time=10ms TTL=128
Reply from 192.168.0.155: bytes=32 time<10ms TTL=128
Reply from 192.168.0.155: bytes=32 time<10ms TTL=128
Reply from 192.168.0.155: bytes=32 time<10ms TTL=128
```

2.1.2 DHCP Enabled PC

If your PC is set to use DHCP, you need to check out IP address of your PC using ' ipconfig' command at DOS Prompt window.

You need to get IP address from your network administrator to assign it to FlexWATCH^{TM} server. IP address should be Surplus of IP address which will be not randomly assigned to any network device in your network.

Your network administrator must make sure that IP address should be excluded from IP pool when he configure Router.

```
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com EtherLink III
ISA (3C509/3C509) in Legacy mode
        Physical Address. . . . . . . . . : 00-60-08-3C-40-90
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.158
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 168.126.63.1
                                  168.126.63.2
        C:\>
```

2.2 LAN cable or Cross-Over Cable

Check out whether FlexWATCH^{TM} server can be connected through LAN cable or Cross--

over cable.

2.2.1 LAN Cable Environment

If your PC is connected to network through LAN cable, you need to connect FlexWATCH^{TM} server to LAN port of Hub or Router.

2.2.2 Cross-over cable

If LAN network is not available, you can directly connect FlexWATCH^{TM} server to your PC through Cross-over cable. In this case, you need to prepare Cross-over cable separately (Note that The LAN cable included in the product package is not Cross-over cable, but normal straight cable) and you need to set your PC IP address as 10.20.30.41 and connect the server with Factory default IP address, 10.20.30.40 through web browser.

Following is brief procedure to connect the server after changing PC IP address.

1) Click right button of your mouse on the 'My Network Places' icon in the main screen window.

2) Click right button of your mouse on the 'Local area connection' icon and select 'Property' option.

3) Select 'Internet protocol (TCP/IP)' option and click 'Property' icon.

4) Select 'use the following IP address' option from the TCP/IP property option and set the IP address as follow

- **IP address : 10.20.30.41**
- **Network Mask : 255.255.255.0**

5) Connect FlexWATCH^{TM} server using Cross-over cable to your PC and run your web browser and enter default IP address, 10.20.30.40 of FlexWATCH^{TM} server in the URL field. Note that Cross-over cable is not supplied with product.

6) Once you are connected to the server, click Admin icon and click LAN configuration menu.

7) Enter IP address you would like to assign to the FlexWATCH^{TM} server and change your PC IP address again.

2.3 PC Environment

Check out whether your PC is connected to LAN or WAN network or stand-alone. If stand alone, you need to use Cross-over cable or build up LAN environment to use LAN cable.

3 Factory Default

Please refer to the following factory defaults to change setting up.

	Factory Default
Admin ID	root
Admin password	root
IP address	10.20.30.40
Network mask	255.255.255.0

4 IP Assignment

FlexWATCH^{TM} server can be configured by two different configuration method and following is brief explanation.

Installation Wizard Program:

IP installation program is provided in CD form. Once FlexWATCH^{TM} server is connected to LAN network, you can assign IP address through program and access the Web browser

HyperTerminal mode:

If no network is available and you want to set up IP address, you can directly connect FlexWATCH^{TM} server to your PC through Serial cable provided together with product. HyperTerminal mode is very useful tool to recover Admin password when you lost your admin password or to report any problem to Manufacturer when product is on malfunction status.

4.1 Through Installation Wizard Program

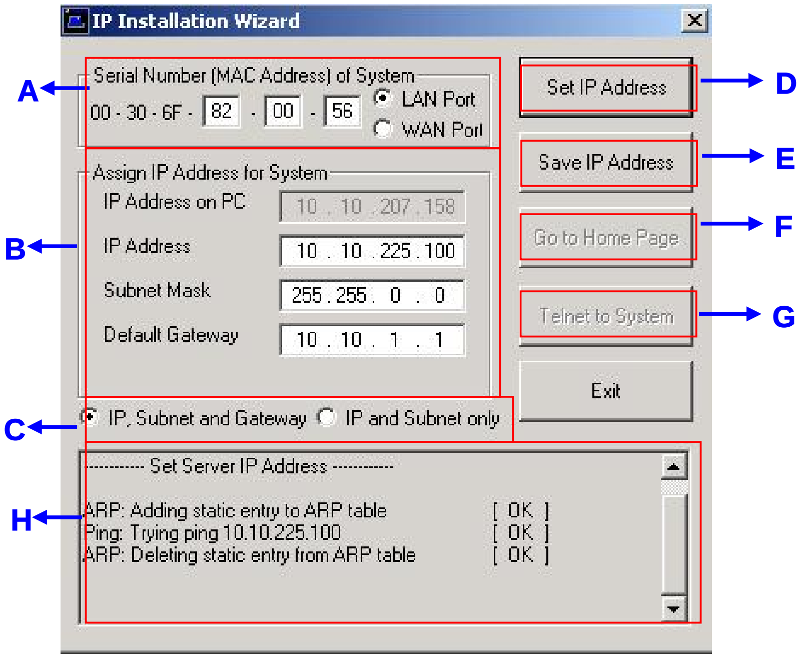
IP setting with Installation Wizard program is easy and simple way and after IP setting is done you can do other configuration through web browser.

You can use **IP Installation Wizard Program** through following step.
(**IPInstallationWizard.exe is provide in the product CD**)

Preset a PC with Microsoft Windows O/S.

1) Connect FlexWATCH^{TM} server into the network (Hub) that your PC belongs to.

2) Run the IP installation Wizard program in your PC. Then following IP Installation Wizard window will show up.



Serial Number (MAC Address) of System
00 - 30 - 6F - 82 - 00 - 56
● LAN Port
○ WAN Port

Assign IP Address for System
IP Address on PC: 10 . 10 . 207 . 158
IP Address: 10 . 10 . 225 . 100
Subnet Mask: 255 . 255 . 0 . 0
Default Gateway: 10 . 10 . 1 . 1

● IP, Subnet and Gateway ○ IP and Subnet only

```
---------- Set Server IP Address ----------

ARP: Adding static entry to ARP table          [ OK ]
Ping: Trying ping 10.10.225.100                [ OK ]
ARP: Deleting static entry from ARP table      [ OK ]
```

Description of Window

	Menu	**Description**
A	**Serial No. (MAC Address)** of System	Enter FlexWATCH^{TM} server Serial No. (Mac address) attached at the bottom of the unit and select the LAN port. WAN PORT is only for setting up FW-5000 and FW-5440 model which has two LAN Card inside of the box.
B	IP Address on PC	*Auto scanned IP address of user's computer with IPInstallationWizard.exe running on.*

	IP Address	Input an IP address to be assigned to FlexWATCH^{TM} server Note that the IP must be directly connectable with user's PC. The above IP **'10.10.225.100'** is only an example.
C	IP, Subnet, Gateway	Whether to change IP, Subnet and Gate or IP and Subnet mask only.
D	'***Set IP Address'*** Button	To activate a new IP assignment, click this button.
E	'**Save IP Address'** Button	To save IP-Address in the Flash Memory.
F	'**Go to Home Page'** Button	To launch FlexWATCH Web browser and start other configuration through Administration page.
G	'Telnet to System' Button	To guide you Telnet mode for Advanced Configuration.
H	Result window	Show the result of IP assignment. If failed, try again from the start or use other configuration method

3) Input the Serial No. (MAC address) and Select "LAN Port".

4) Input the IP address, which will be assigned to the system.

5) Click "Set IP Address" button to save the above configuration.

6) Check whether message type is correctly appeared on Result window as below.

```
------------ Set Server IP Address ------------

ARP: Adding static entry to ARP table            [  OK  ]
Ping: Trying ping 10.10.225.100                  [  OK  ]
ARP: Deleting static entry from ARP table        [  OK  ]
```

7) If message come up as below, IP address setting has been failed.

```
------------ Set Server IP Address ------------

ARP: Adding static entry to ARP table            [  OK  ]
Ping: Trying ping 10.10.225.100                  [FAILED]
    Please check whether IP address and MAC address is
valid.
    Then, please retry again.
ARP: Deleting static entry from ARP table        [  OK  ]
```

- If IP address setting is failed, please check whether correct IP/MAC address is entered. And try again with correct IP/MAC address, or please use HyperTerminal method.
- If the above result is O.K., follow the next step to finish Network Configuration.

8) Click "Save IP Address" button to save IP-Address in the Flash Memory.

9) Click "Go to Home Page" button to access to FlexWATCH^{TM} Web browser.

10) For server configuration, click "**Admin**" Icon and Input User ID and Password (Factory default is **root : root**) to get into configuration mode and then press "OK" button.

☞ ***Note***

Once you changed the IP address of FlexWATCH^{TM} server, you need to connect the server with the changed IP address. If you lost the IP address assigned to FlexWATCH^{TM} server, you need to set-up a new IP address again.

☞ ***Note***

If IP address set result is failed, please check whether correct IP/MAC address is entered. And try again with correct IP/MAC address, or please use HyperTerminal method.

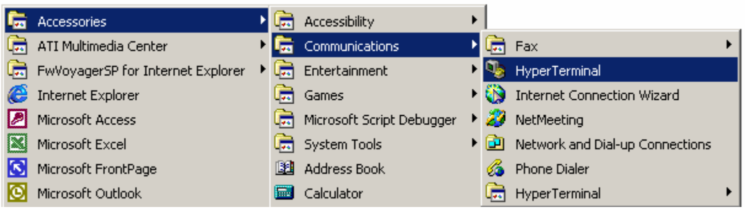
4.2 IP Assignment through Hyper Terminal mode

Microsoft Windows provides Terminal emulation program, namely Hyper Terminal. For HyperTerminal connection, Power, RS-232 Cable and LAN cable must be connected to FlexWATCH^{TM} server with user's PC. LAN cable is to run Web browser after configuration using HyperTerminal. You can continue the below configuration after Network setting and the next process will be same as using Installation Wizard Program.

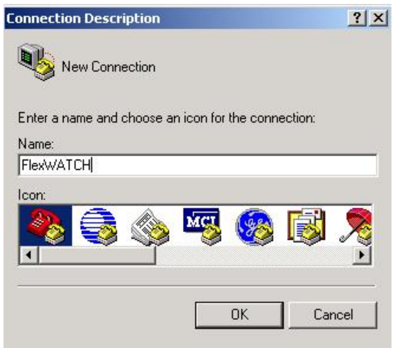
1) Link up with the provided serial cable between COM port at FW-3440 and COM1 or COM2 at user's PC.

2) Run Hyper Terminal Program on user's PC.

Window start> Program> Accessories> Communication> Hyper Terminal


Accessories
ATI Multimedia Center
FwVoyagerSP for Internet Explorer
Internet Explorer
Microsoft Access
Microsoft Excel
Microsoft FrontPage
Microsoft Outlook
Accessibility
Communications
Entertainment
Games
Microsoft Script Debugger
System Tools
Address Book
Calculator
Fax
HyperTerminal
Internet Connection Wizard
NetMeeting
Network and Dial-up Connections
Phone Dialer
HyperTerminal

3) If Hyper Terminal window come up as below, input HyperTerminal name (ex. Flexwatch) and press 'OK' button.


Connection Description
OK
Cancel

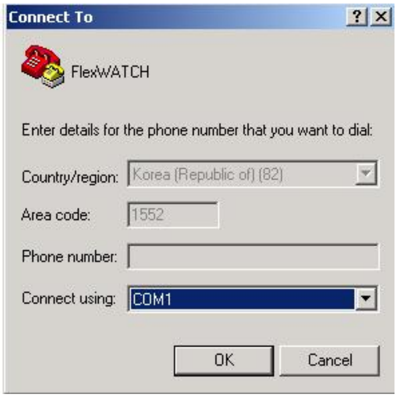
New Connection

Enter a name and choose an icon for the connection:

Name: FlexWATCH

Icon:

4) Select the connected COM port with serial cable and press OK button.


Connect To
OK
Cancel

FlexWATCH

Enter details for the phone number that you want to dial:

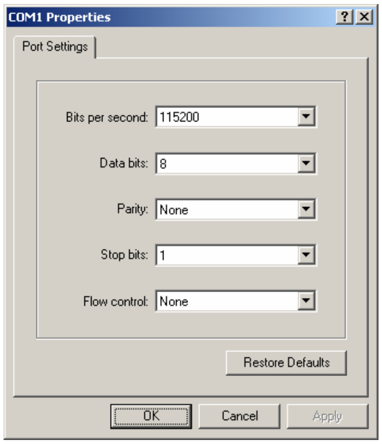
Country/region: Korea (Republic of) (82)

Area code: 1552

Phone number:

Connect using: COM1

5) When 'Port Settings' window show up, input each values from the table below.


COM1 Properties
Port Settings
Restore Defaults
OK
Cancel
Apply

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Serial Port Settings	Value
Bits per Second	**115200**
Data bits	**8**
Parity	**None**

Stop bits	**1**
Flow control	**None**

6) After setting Hyper Terminal, press Enter key several times and then you can see messages as below. Input Login ID and Password. (Factory defaults for Admin ID and Password are root/root.)

```
Seyeon Tech Co., Ltd. 2001-2003
Linux Kernel 2.4.20-syl1

FlexWATCH login:
```

7) If you correctly input Login ID and Password, 'bash#' prompt will show up as below.

```
FlexWATCH login: root
Password:


 ----------------------------------------------------------
 SYSTEM      : FlexWATCH
 VERSION     : 3.0.040130
 MODEL       : FW-3110
 ----------------------------------------------------------


login[504]: root login  on `ttyS0'

bash#
```

8) Input '**netconfig**' command after 'bash# ' prompt, and press Enter key. Then you can see following network setup values.

```
bash# netconfig

-------------------- Network(LAN) Setup --------------------

Current configuation
       IP Address   : 10.20.30.40
       Network Mask : 255.255.255.0
       Gateway      : 10.10.1.1

Enter IP Address   :
```

9) Input new IP address, Network Mask and Gateway values to be assigned to FlexWATCH^{TM} server. After this, press "y" to apply the new network configuration.

```
Enter IP Address   : 10.10.213.22
Enter Network Mask : 255.255.0.0
Enter Gateway      : 10.10.1.1

Entered network configuation
       IP Address   : 10.10.213.22
       Network Mask : 255.255.0.0
       Gateway      : 10.10.1.1.

Do you wish to apply your new network configuration ?
(y/n/q): y
```

10) If following messages come up on your screen with "bash# " prompt, the new network configuration has successfully applied.

```
Your network configuration was changed.
Shutting down interface eth0 [  OK  ]
Shutting down interface ppp1 [  OK  ]
Shutting down interface ppp2 [  OK  ]
Setting network parameters [  OK  ]
Bringing up interface lo [  OK  ]
Bringing up interface eth0 eth0: Setting half-duplex based on auto-negotiated partner ability 0000.
[  OK  ]
Bringing up interface ppp1 [  OK  ]
Your new network configuration was applied.
bash#
```

11) To check whether your Network configuration is correctly applied or not, press '**ifconfig**' command after "bash#" prompt and then following messages will show up. On the second line of the 'eth0' message, you can check the assigned IP and Mask values. Gateway value is not seen here. If the values are different from what you want to set-up, try again the Network configuration from step 8**)**.

```
Bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:30:6F:81:00:AE
          inet addr:10.10.213.22  Bcast:10.10.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6382 errors:0 dropped:0 overruns:0 frame:0
          TX packets:294 errors:0 dropped:0 overruns:0 carrier:0
          collisions:2 txqueuelen:100
          Interrupt:9

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

bash#
```

12) Input ‘**savecfg**’ command to save the changed configuration to Flash Memory. And Input ‘reboot’ command to reboot the system.

```
bash#
bash# savecfg
Saving a current config to flash memory
[  OK  ]
Updated flash
bash#
bash#
bash# reboot

Broadcast message from root (ttyp0) Mon Sep  6 19:28:51
2004...

The system is going down for reboot NOW !!
bash#
```

Live view & Camera Configuration

Once IP assignment is finished, you can view live view through standard web browser such as MS Internet Explorer or Netscape Navigator.

There are two different type of viewing option provided by FlexWATCH^{TM} server. One is simple live view and the other is "***FW-Voyager***" which provides personal Network DVR(Digital Video Recording) and viewing solution.

Depending on the OS and web browser, you can get different viewing option as well. Following is guide for OS and Web browser for live view.

Viewing mode	**Operation System**	**Web browser**
Simple view (ActiveX)	MS Window	Internet explorer only
Java Applet mode	Window, Linux, Unix, MAC, OS2	Netscape and other web browser
FW-Voyager (Recording)	MS Window	Internet Explorer only

* Note that FlexWATCH^{TM} server supports only Internet Explorer or Netscape Navigator. No additional support will be given to support any specific web browser except above.

1 Live View

Video server is designed to automatically sense the OS of Client PC and Web browser. Depending on the OS and web browser it provides different option such as ActiveX and Java Applet.

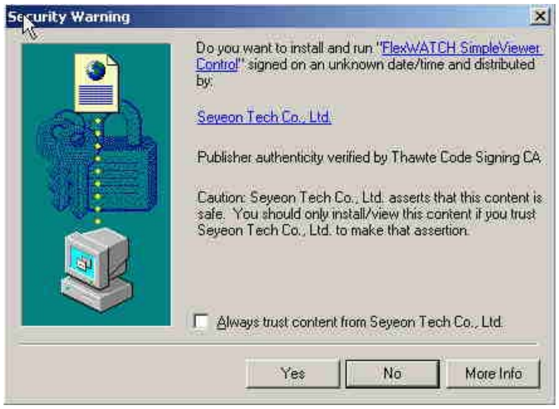
1.1 ActiveX based simple view

This mode is to view live through **Internet explorer on the MS Window**

Small ActiveX components should be automatically installed or manually installed in the client PC to view live if Client PC use Internet explorer on the MS Window.

When the client pc is connected to internet, ActiveX components will automatically downloaded and installed in the view PC if you accept to download and install [FlexWATCH^{TM} **Simple Viewer control**] program

- Click "**Live view**" tab in the web browser
- Click "**Yes**" button when security Warning panel come up
- Then, live view will be displayed



Security Warning

Do you want to install and run "FlexWATCH SimpleViewer Control" signed on an unknown date/time and distributed by:

Seyeon Tech Co., Ltd.

Publisher authenticity verified by Thawte Code Signing CA

Caution: Seyeon Tech Co., Ltd. asserts that this content is safe. You should only install/view this content if you trust Seyeon Tech Co., Ltd. to make that assertion.

☐ Always trust content from Seyeon Tech Co., Ltd.

When the Client pc is not connected to Internet, you need to manually install ActiveX components in your viewing PC.

- Insert the product CD in your PC
- Select "FlexWATCH^{TM} Simple Viewer control" program
-

Application idea

ActiveX based SDK is provided for software developers so that application program developers can easily utilize digital video from FlexWATCH^{TM} server for his own video application.

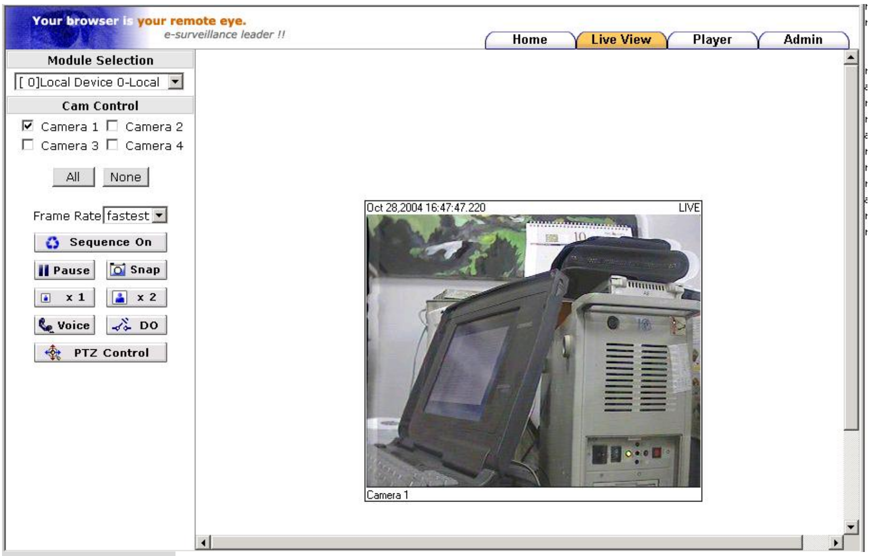
1.2 Java Applet based live view

Java applet is to display live video through any web browser on any Operating system supporting Java Virtual Machine. This is to view live video through **Netscape navigator on MS window** or other Operation system such as **Unix, Linux, MAC and OS2**. Thus, if you are using MS IE on MS Window, Java Applet can not be enabled.

Note that JRE(Java Runtime Environment) must be running in your web browser to display live video on Unix, Linux, Mac, OS2 Operating system or Netscape Navigator on Window. If not, you need to manually download and install JRE file from the web page of Sun Microsystems.

1.3 Live view page guide

Simple viewer page provides various control option such as image magnification, full screen, snapshot, PTZ control, Relay output control, Voice kit connection as well.


Your browser is your remote eye.
e-surveillance leader !!
Home
Live View
Player
Admin
Module Selection
[0]Local Device 0-Local
Cam Control
☑ Camera 1 ☐ Camera 2
☐ Camera 3 ☐ Camera 4
All
None
Frame Rate fastest
Sequence On
Pause
Snap
x 1
x 2
Voice
DO
PTZ Control
Oct 28,2004 16:47:47.220
LIVE
Camera 1

Cam Control :
By checking the camera you can get any number of camera displayed on the same screen. Camera 1, 2, 3, 4 and all cameras can be displayed together.

Sequence :
To view camera selected camera sequentially.

Frame rate :
You can adjust display frame rate by control Frame rate option

Display size :
X1 for Real size, x2 for double size and Full screen mode is supported.

Snap shot :
You can make a snapshot of video while viewing the live video.

Voice :
When the voice kit, FW-V10S is connected to the FlexWATCH^{TM} server, you can simultaneously listen and speak with your counter part through web browser.

PTZ :
PTZ(pan/tilt/zoom) device can be controlled through web browser. When click "PTZ" button, PTZ control panel will separately be appeared. But note that you need to get permission to control it.

Output control :

Relay output device can be controlled through simple view page. But note that you need to get permission to control it.

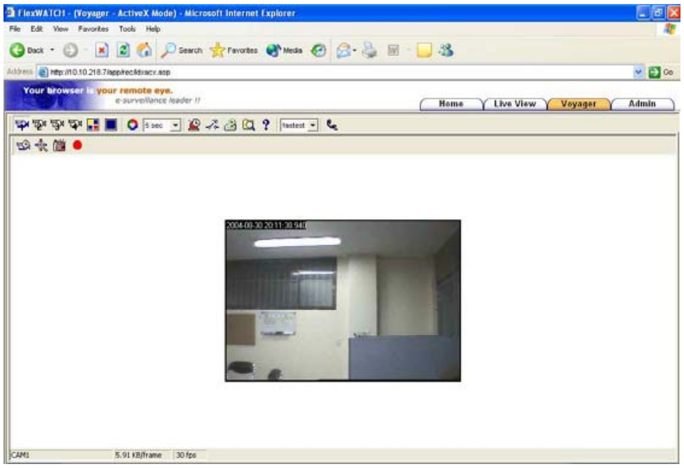
2 FW-Voyager based view and recording

FW-Voyager is web based DVR software for personal video recording. Using this free software, user can easily install the software and do video recording at any time.

Note that FW-Voyager is works on MS Internet explorer of Window OS.

- Click “Voyager” tab in the web page of the server
- Wait till the Voyager program is automatically downloaded.
- Click “yes” in the Security warning panel
- Then software will automatically installed.

For the operation of the software, please refer to user guide of FW-Voyager software included in the product CD.


FlexWATCH - (Voyager - ActiveX Mode) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://10.10.218.7/app/rec/drxacx.asp
Go
Your browser is your remote eye.
e-surveillance leader !!
Home
Live View
Voyager
Admin
5 sec
fastest
2004-08-30 20:11:30.940
CAM1
5.91 KB/frame
30 fps

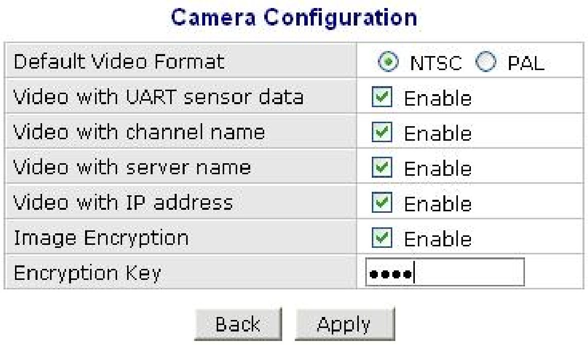
3 Camera configuration

This is to configure camera related settings such as camera value string and video quality setting.

3.1 Camera value string configuration

Some of video related value string can be

transmitted along with live video stream so that client program can receive and utilize video related value string for his own application.



Camera Configuration

Default Video Format	● NTSC ○ PAL
Video with UART sensor data	☑ Enable
Video with channel name	☑ Enable
Video with server name	☑ Enable
Video with IP address	☑ Enable
Image Encryption	☑ Enable
Encryption Key	●●●●

Default Video Format :

To manually change video format. Note that server auto sense the video format

Video with UART sensor data:

Serial input data can be sent along with video so that application program can read serial input data

Video with channel name:

To send video along with channel name

Video with server name:

To send video along with server name

Video with IP address:

To send video along with IP Address

Image encryption:

Image encryption is security feature. Once it is enabled, user must enter encryption code to view live video.

Note

All of video related values are encrypted in the JPEG image and can not be read by any program as it is. It is intended to help application program developer to utilize video related value string for his own specific application. Manufacturer can provide more technical documentation for the programmer to decrypt value string for his programming.

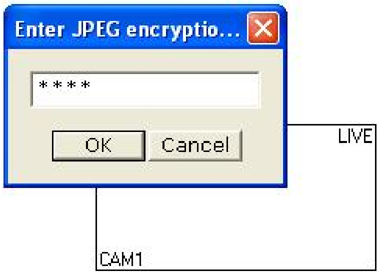
Thus, please contact your local vendor to get more in-depth technical info to decrypt the value string.

3.1.1 Image encryption

Image encryption is security feature to prevent unwanted image hacking when anonymous user accesses the system. Once it is enabled, user must enter encryption code to view live video.

1) Simple set up encryption code

2) Enter encryption key code to view live. Up to 8 alpha-numeric characters can be used.



☞ ***Note***

Once you lost your encryption code, you can reconfigure encryption code through Admin Mode.

Once Image encryption is enabled, FW-Manager can not display live video. Thus, you must disable Encryption mode when the image is to be viewed from FW-Manager program.

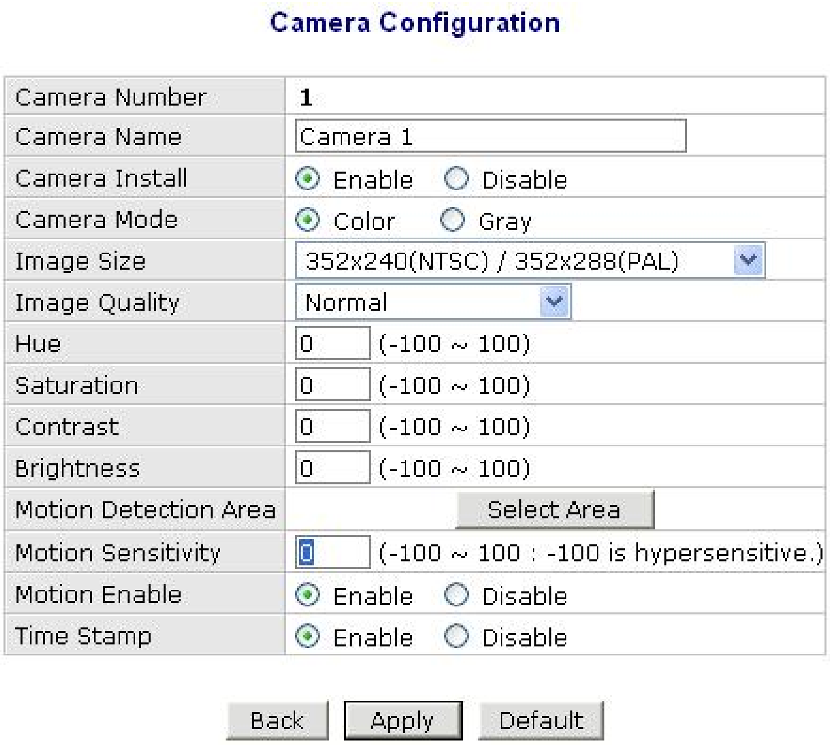
3.2 Camera configuration

Through camera configuration mode, you can adjust the video quality to meet your requirement.

1) Click '**Camera configuration'** menu in the Service configuration mode of admin window

2) Set up camera value string

3) Select Camera channel and set up camera related information such as Camera name and quality setting.



Camera Configuration

Camera Number	1
Camera Name	Camera 1
Camera Install	● Enable ○ Disable
Camera Mode	● Color ○ Gray
Image Size	352x240(NTSC) / 352x288(PAL)
Image Quality	Normal
Hue	0 (-100 ~ 100)
Saturation	0 (-100 ~ 100)
Contrast	0 (-100 ~ 100)
Brightness	0 (-100 ~ 100)
Motion Detection Area	Select Area
Motion Sensitivity	0 (-100 ~ 100 : -100 is hypersensitive.)
Motion Enable	● Enable ○ Disable
Time Stamp	● Enable ○ Disable

User defined camera name will be appeared on the camera name column of video. Up to 20 different English characters can be used.

(Notice : If you are using 2-Byte Unicode Character, number of character is limited to 10)

Image Size : 4 different size of video can be set up.

	Full	Large	Normal	Small
NTSC	704 x 480	704 x 240	352 x 240	176 x 112
PAL	704 x 576	704 x 288	352 x 288	176 x 144

Application Idea

Full size of video can show interlaced video when the camera is displaying fast moving picture. To avoid interlaced video, use large size of video which use Field image only. Note that in this case, camera quality can slightly be degraded..

Channel install :

Whether to enable video channel or not. If "Disable" is selected, camera will not be displayed.

Video Source: color and Gray mode option

Image Quality: 5 quality levels - highest, high, normal, low, lowest

☞ ***Note***

Please note that if you increase image size and quality, actual JPEG file size will be increased and this may affect actual transmission frame rate. Thus, you are required to check out your network bandwidth available for FlexWATCH™ server and select the right size and quality of video.

Motion Detection : Refer to description about Motion detection feature below.

Time stamp : Date and Time information can be engraved in the JPEG Image. It is recommended to use time stamp only when you need image with built-in time info.

☞ ***Note that once Time stamp is enabled, over all transmission speed can be degraded.***

3.3 Video Motion Detection

Built-in motion detection function is supported by the FlexWATCH™ server so that server can sense the motion in the picture and trigger any services such as e-mail, FTP or alarm buffering services.

Up to 144 square blocks can be configured as a motion area so that you can flexibly filter out motion area.

3.3.1 Setting procedure

1) Go to "**Camera & Motion**" option in the Admin Menu

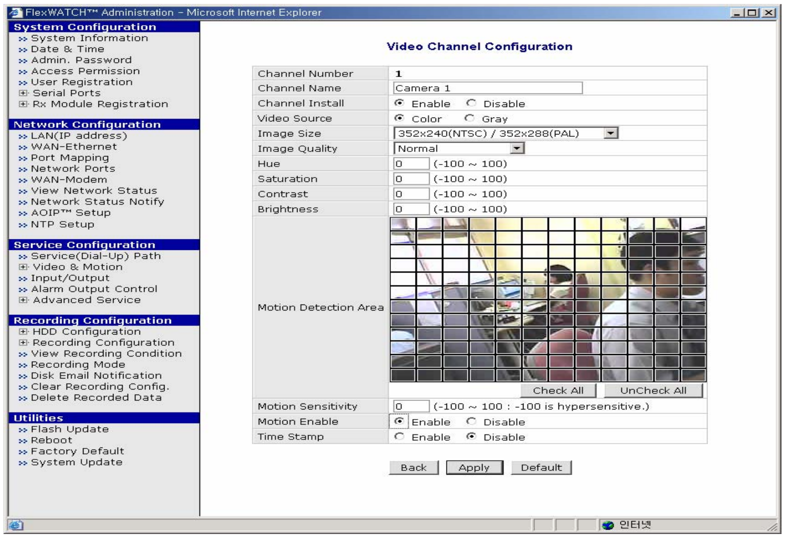
2) Select the camera for video configuration

3) Click "**Select Area**" button from the Camera configuration menu

4) Click the **square block** to set up motion detection area

5) Adjust Motion sensitivity (**the lower the number, the higher the motion sensitivity**)

6) Check "**Motion Enable**" check box and Click "**Apply**" button to save your configuration


FlexWATCH™ Administration - Microsoft Internet Explorer
System Configuration
System Information
Date & Time
Admin. Password
Access Permission
User Registration
Serial Ports
Rx Module Registration
Network Configuration
LAN(IP address)
WAN-Ethernet
Port Mapping
Network Ports
WAN-Modem
View Network Status
Network Status Notify
AOIP™ Setup
NTP Setup
Service Configuration
Service(Dial-Up) Path
Video & Motion
Input/Output
Alarm Output Control
Advanced Service
Recording Configuration
HDD Configuration
Recording Configuration
View Recording Condition
Recording Mode
Disk Email Notification
Clear Recording Config.
Delete Recorded Data
Utilities
Flash Update
Reboot
Factory Default
System Update
Check All
UnCheck All
Back
Apply
Default
인터넷

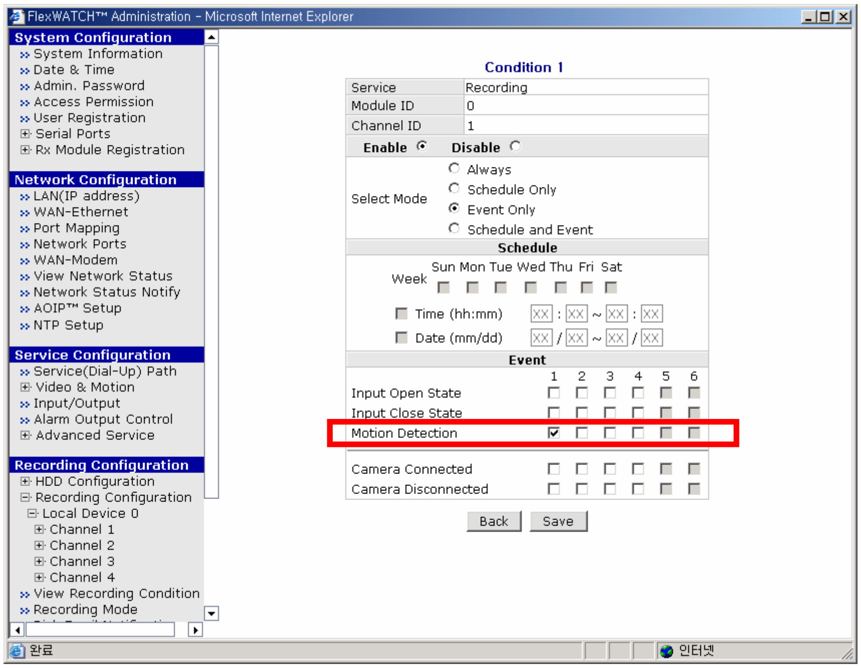
Video Channel Configuration

Channel Number	1
Channel Name	Camera 1
Channel Install	● Enable ○ Disable
Video Source	● Color ○ Gray
Image Size	352x240(NTSC) / 352x288(PAL)
Image Quality	Normal
Hue	0 (-100 ~ 100)
Saturation	0 (-100 ~ 100)
Contrast	0 (-100 ~ 100)
Brightness	0 (-100 ~ 100)
Motion Detection Area	
Motion Sensitivity	0 (-100 ~ 100 : -100 is hypersensitive.)
Motion Enable	● Enable ○ Disable
Time Stamp	○ Enable ● Disable

3.3.2 How to save Motion triggered image in the NVR solution

Recording in the FW-5440/5000

Simply check "**Motion Detection**" option in the recording condition menu in the FW-5440 or FW-5000 when motion detection option is enabled in the FlexWATCH^{TM} server.


FlexWATCH™ Administration - Microsoft Internet Explorer
System Configuration
System Information
Date & Time
Admin. Password
Access Permission
User Registration
Serial Ports
Rx Module Registration
Network Configuration
LAN(IP address)
WAN-Ethernet
Port Mapping
Network Ports
WAN-Modem
View Network Status
Network Status Notify
AOIP™ Setup
NTP Setup
Service Configuration
Service(Dial-Up) Path
Video & Motion
Input/Output
Alarm Output Control
Advanced Service
Recording Configuration
HDD Configuration
Recording Configuration
Local Device 0
Channel 1
Channel 2
Channel 3
Channel 4
View Recording Condition
Recording Mode
Back
Save
완료
인터넷

Condition 1

Service	Recording
Module ID	0
Channel ID	1
Enable ●	**Disable** ○
Select Mode	○ Always ○ Schedule Only ● Event Only ○ Schedule and Event

Schedule

Week: Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐

☐ Time (hh:mm) XX : XX ~ XX : XX

☐ Date (mm/dd) XX / XX ~ XX / XX

Event

	1	2	3	4	5	6
Input Open State	☐	☐	☐	☐	☐	☐
Input Close State	☐	☐	☐	☐	☐	☐
Motion Detection	☑	☐	☐	☐	☐	☐
Camera Connected	☐	☐	☐	☐	☐	☐
Camera Disconnected	☐	☐	☐	☐	☐	☐

Recording in the FW-Manager

To record motion triggered image in the FW-Manager (NDVR Software) client program, you **should not use Software motion detection function in the FW-Manager.**

- **Simply configure motion detection for the selected camera in the FlexWATCH^{TM} server**
- **Set up Motion based recording condition in the FW-Manager (Do not set up motion detection area in the FW-Manager software).**

System Configuration

System configuration is to set up basic functions which help you properly run and manage the system. It is highly recommended to set up the configuration before any other configurations. Following functions are provided in the System configuration mode.

- **System name and Info**
- **System Administration account set up**
- **System access level setting**
- **Serial port configuration (PTZ or external device connection)**
- **TX Module configuration**

1 System Information

System information is very important one

Following menu will be provided

Server Name	User definable and Identifier of the system when the system is accessed by third party program such as NDVR software**.**
Serial Number	Product serial number. This information must be **submitted for RMA or Warranty claim**
Model	This information also needs to be submitted for **technical support request**
Version	System firmware version. This information also needs to be **submitted for technical support request**

2 Date & Time

Date & time is very important factor to trigger any service at the right time such as FTP, e-Mail, Alarm notification etc. **If Date & time is not correctly set up in the system, any service which will be triggered by schedule condition will be not done correctly.**

Also Server Date & time info will be displayed on the image. If you need to display correct time, please set up more accurate time information.

2.1 Date & Time in the server clock

Date & time can be set up in the real time clock built in the server. Simple set up Date & Time info in the Date & Time configuration field.

1) Go to Date & Time setup menu in the System configuration section of Admin mode
2) Set the correct time and click "Apply" button

2.2 Date & Time using NTP server

If multiple servers are installed over the network and controlled by client program and synchronized time info is required, use NTP(Network Time Protocol) option.

1) Go to [**NTP setup**] menu in the Network configuration section of Admin Mode
2) Type in NTP server name or use default NTP timeserver, **ntp.ewha.net,** if you do not know any NTP timeserver available in your area.

☞ ***Note***

NTP timeserver provides exact time wherever it is located.

3) Enable the service and select **Time Zone** where **the FlexWATCH™ server is located** (not user's viewing pc area)
4) Type in NTP timeserver info.

3 Admin Password Setup

System administration Menu is user definable. It is highly recommended to change default Admin Password to prevent any unwanted server control by any other person.

☞ ***Please note followings***

A. Factory default admin ID is *root* and Password is *root* (Case sensitive)
B. Admin ID(root) is not user definable and unchanging
A. Only Admin Password is user definable

4 Access Control and User registration

Access permission is to set up user account for the system access. Through this configuration you can create multiple user account with **different control authority for each camera** and edit or delete user account.

Following features are provided by this mode

A. Option to allow system access without system Login ID & PW

B. Channel based different user account creation

C. Different control authority for Video, PTZ, Audio, and relay output device control

4.1 Full Access

To allow **system access by anyone** who know the IP address. PTZ, Audio and Relay output device can be controlled by anyone. Thus, if security for video is important, it is highly recommended to user limited access mode below

4.2 Limited Access and User registration

This is to limit server access to the authorized user only. Through this mode, you can create multi level access account for each camera, not system level, with different control authority.

Once Limited Access option is selected, User registration should be followed to effectively use Limited Access function.

☞ ***Application Tips***

If **servers are accessed and controlled by third party application program** and if you want to give different control authority for each camera to different application program, you can give different access and control authority for PTZ, Audio, Relay output device control for specific camera by creating different User account in the server.

Following is step for Limited access account for each camera.

1) Select [**Limited Access**] option in the Access Permission menu

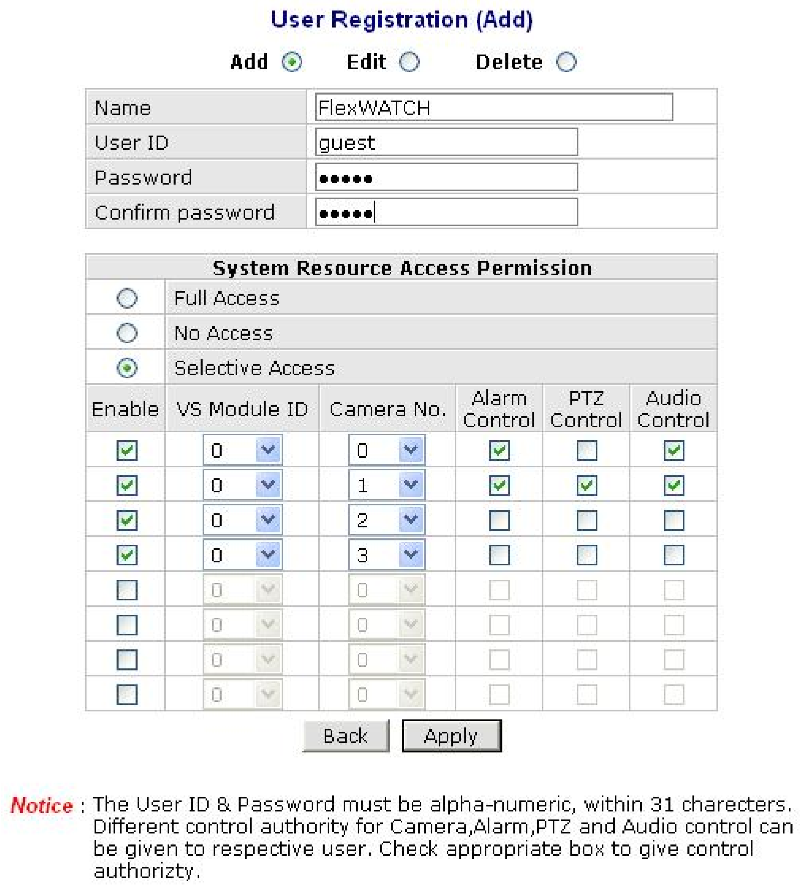
2) Click [**Apply**] button

3) Click [**user registration**] menu in the System configuration section of Admin window

4) Fill out the column provided such as User name, ID & Password

5) Select the Camera module for which you would like to give permission and check control item such as Alarm control, PTZ, and Audio control.

☞ ***Note default VS Module ID is 0 and only Default VS Module ID is workable.***



User Registration (Add)

Add ● Edit ○ Delete ○

Name	FlexWATCH
User ID	guest
Password	●●●●●
Confirm password	●●●●●

System Resource Access Permission

○ Full Access

○ No Access

● Selective Access

Enable	VS Module ID	Camera No.	Alarm Control	PTZ Control	Audio Control
☑	0	0	☑	☐	☑
☑	0	1	☑	☑	☑
☑	0	2	☐	☐	☐
☑	0	3	☐	☐	☐
☐	0	0	☐	☐	☐
☐	0	0	☐	☐	☐
☐	0	0	☐	☐	☐
☐	0	0	☐	☐	☐

Notice : The User ID & Password must be alpha-numeric, within 31 charecters. Different control authority for Camera,Alarm,PTZ and Audio control can be given to respective user. Check appropriate box to give control authorizty.

Full Access :

If full access is selected, any body can access the server and control the video.

No Access :

This is to temporally restrict camera access by specific user without delete user account to temporally block access to the camera.

Selective Access:

This is to set up control authority for the respective or all cameras.

VS Module ID is FlexWATCH^{TM} server ID which is recognized by the server. Default # is 0.

Please disregard other VS Module ID appeared in the drop down menu. Other module numbers is for future use which is not currently workable.

Camera number start from 0 which is the first camera connected to BNC connect #1.

Thus, 4^{TH} camera can be Camera# 3 in this menu.

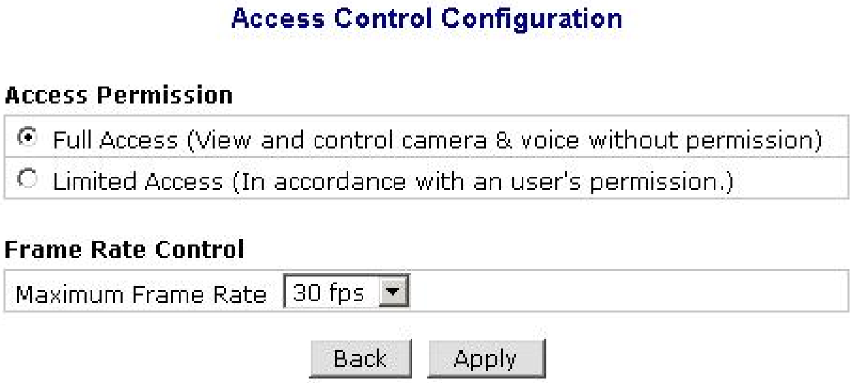
5 Frame rate control

Maximum Video frame rate which sever can transmit over the IP network can be set up through Frame rate control option. Through this maximum frame rate control option, user can limit network bandwidth consumption by video transmission.

1) Go to [**Access Control**] option in the system configuration menu in the Admin page.

2) Set up Maximum frame rate. Following table could be an example.

File size is variable depending on the complexity of the scene. Thus, it hard to get exact and fixed number of file size.



Access Control Configuration

Access Permission

● Full Access (View and control camera & voice without permission)

○ Limited Access (In accordance with an user's permission.)

Frame Rate Control

Maximum Frame Rate: 30 fps

Frame rate requirement

Format	Resolution	Average File size	Required Bandwidth	
			10FPS	25FPS
NTSC	176X112	3KBps	240K bps	600K bps
	352X240	8KBps	640K bps	1.6M bps
	704X480	20KBps	1.6M bps	4M bps
PAL	173X114	4KBps	320K bps	800K bps
	352X 288	10KBps	800K bps	2.0M bps
	704X 576	25KBps	2M bps	5M bps

***** Above file size table is average file size manufacture got from the lab test.

Formula to calculate required Bandwidth

File Size x FPS X 8 bits

3) Click [**Apply**] button

6 Tx Module Registration(NVCP)

☞ **Notice**

- If you do not connect FlexWATCH™ server to NDVR server, do not set TX module configuration
- Once Tx Module configuration is done, set up RX module configuration in the NDVR server as well

Video proxy function is supported by NDVR server such as FW-5440 and FW-5000 server. By registering FlexWATCH™ video server into NDVR server, live video can be recorded in the NDVR server and live view can be accessed through NDVR server web page which means user does not need to separately run web browser to view respective cameras from FlexWATCH™ video servers.

TX module registration is to set up the FlexWATCH™ server to communicate with FW-5440 or FW-5000 NDVR server or FW-VSS Proxy Server only. When TX module is enabled at the FlexWATCH™ server, RX module at NDVR server side should also be enabled as well.

Two different modes are provided as a connection type. One is Passive and the other is Active mode. Depending on which device tries to establish the connection to the other party, the connection type will be decided.

Passive mode : NDVR server tries to establish connection to FlexWATCH™ server
Active Mode : FlexWATCH™ server tries to establish connection to NDVR server

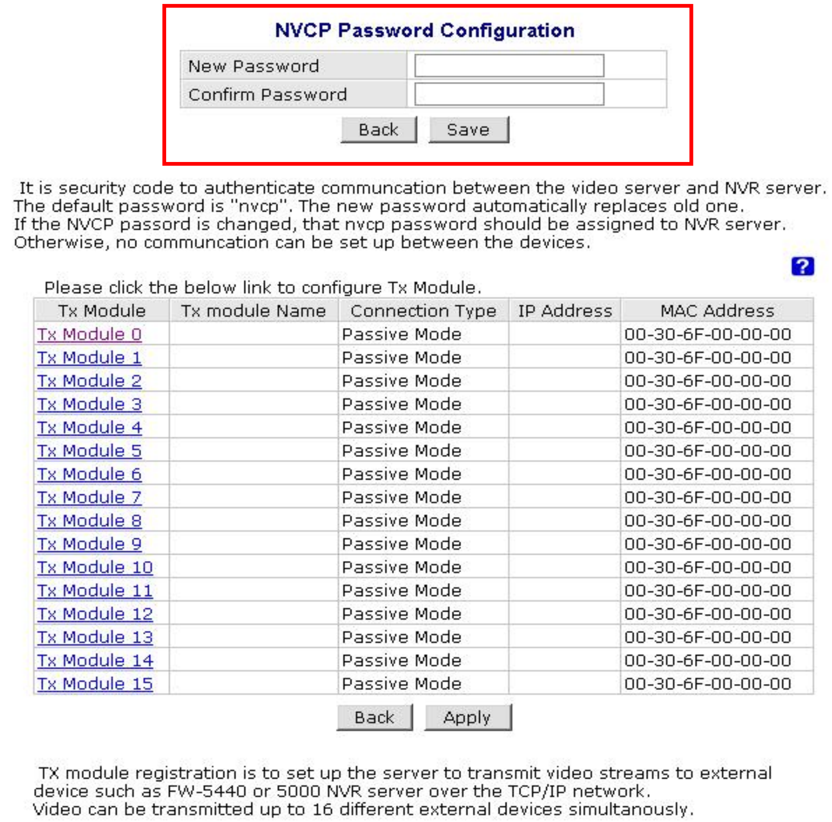
Once connection type is decided in the FlexWATCH™ server, the connection type in the NDVR server should be opposite so that it can communicate with FlexWATCH™ server. For example, once Passive mode is set up in the FlexWATCH™ server, Active mode must be set in the NDVR server.

1) Click TX Module registration menu in the System configuration mode of Admin window.

2) Type in NVCP Password in the NVCP Password configuration filed.

☞ ***Notice***

NVCP Password is security feature which authenticate server access by RX module (FW-5440 or 5000 NDVR server) to FlexWATCH^{TM} server. Once NVCP Password is configured, that password must be set up in the NDVR server to get video from FlexWATCH^{TM} server. Thus, you must make a note of NVCP password.



NVCP Password Configuration

New Password	
Confirm Password	

It is security code to authenticate communcation between the video server and NVR server. The default password is "nvcp". The new password automatically replaces old one. If the NVCP passord is changed, that nvcp password should be assigned to NVR server. Otherwise, no communcation can be set up between the devices.

Please click the below link to configure Tx Module.

Tx Module	Tx module Name	Connection Type	IP Address	MAC Address
Tx Module 0		Passive Mode		00-30-6F-00-00-00
Tx Module 1		Passive Mode		00-30-6F-00-00-00
Tx Module 2		Passive Mode		00-30-6F-00-00-00
Tx Module 3		Passive Mode		00-30-6F-00-00-00
Tx Module 4		Passive Mode		00-30-6F-00-00-00
Tx Module 5		Passive Mode		00-30-6F-00-00-00
Tx Module 6		Passive Mode		00-30-6F-00-00-00
Tx Module 7		Passive Mode		00-30-6F-00-00-00
Tx Module 8		Passive Mode		00-30-6F-00-00-00
Tx Module 9		Passive Mode		00-30-6F-00-00-00
Tx Module 10		Passive Mode		00-30-6F-00-00-00
Tx Module 11		Passive Mode		00-30-6F-00-00-00
Tx Module 12		Passive Mode		00-30-6F-00-00-00
Tx Module 13		Passive Mode		00-30-6F-00-00-00
Tx Module 14		Passive Mode		00-30-6F-00-00-00
Tx Module 15		Passive Mode		00-30-6F-00-00-00

TX module registration is to set up the server to transmit video streams to external device such as FW-5440 or 5000 NVR server over the TCP/IP network. Video can be transmitted up to 16 different external devices simultanously.

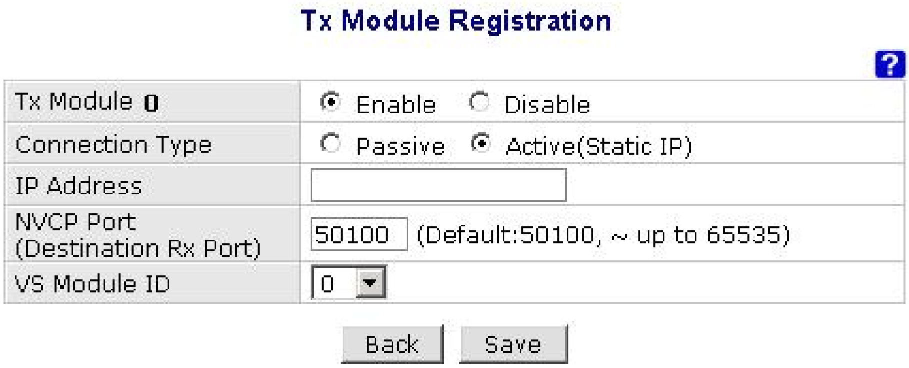
3) Select TX Module. By configuring TX module, you can program the server to communicate with different NVR servers. **Up to16 different NDVR servers** can simultaneously work with FlexWATCH^{TM} server.

4) Select Passive or Active Mode depends on the network situation with NDVR server.

5) Once Active mode is selected, type in IP address of NDVR server.

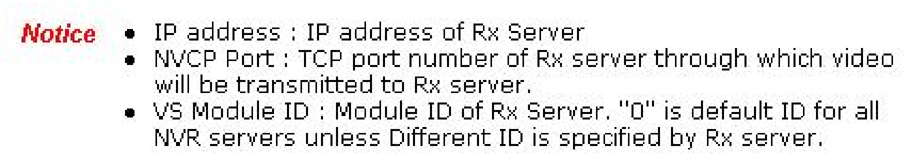
☞ ***Note***

NVCP port should be open to communicate with NDVR Server, when the FlexWATCH™ server is programmed to communication with NDVR server



Tx Module Registration

Tx Module 0	● Enable ○ Disable
Connection Type	○ Passive ● Active(Static IP)
IP Address	
NVCP Port (Destination Rx Port)	50100 (Default:50100, ~ up to 65535)
VS Module ID	0



Notice

- IP address : IP address of Rx Server
- NVCP Port : TCP port number of Rx server through which video will be transmitted to Rx server.
- VS Module ID : Module ID of Rx Server. "0" is default ID for all NVR servers unless Different ID is specified by Rx server.

Following is recommended setting guide for TX and RX module for FlexWATCH™ server and NDVR depending on the network environment

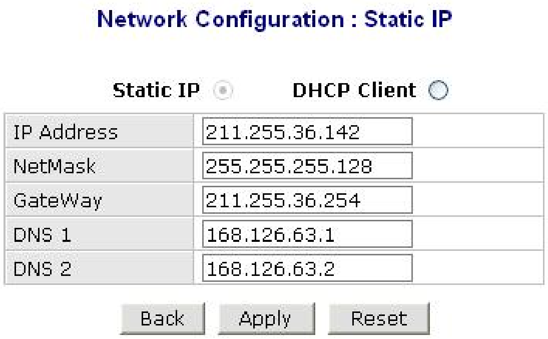
Video server		**NDVR Server**	
Mode	**Network environment**	**Mode**	**Network environment**
Passive mode	WAN Network(Global Static)	**Active Mode**	LAN network (Private)
Passive mode	LAN Network (Private)	**Active mode**	LAN Network (Private)
Active Mode	LAN Network (Private)	**Passive mode**	WAN network (Global Static)
Active Mode	WAN Network(Global Static)	**Passive mode**	WAN Network(Global Static)

Network Configuration

Network configuration mode provides interface for the server to be connected to broadband network or PSTN line. In addition to basic network, application port such as HTTP, NVCP, Voice port configuration and IP filtering options are provided.

1 Network configuration

You can change IP address of server through LAN configuration mode.



Network Configuration : Static IP

Static IP ● DHCP Client ○

IP Address	211.255.36.142
NetMask	255.255.255.128
GateWay	211.255.36.254
DNS 1	168.126.63.1
DNS 2	168.126.63.2

1.1 Static IP

Select this to assign static IP in the server. Subnet mask, Default Gateway information must comply with the network where server is installed. Otherwise, server cannot be connected through network.

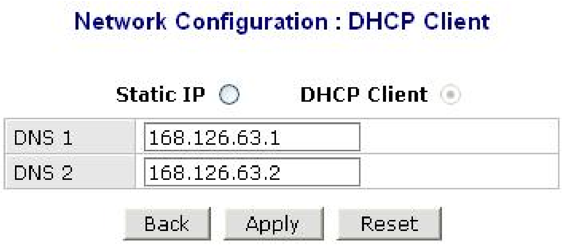
1.2 DHCP Client

This setting is recommended when the server is installed under DHCP environment in the LAN or Cable modem, xDSL Modem which provides PPPOA type service.

We recommend you to use DHCP option when the server is directly connected to Cable modem only.

1.2.1 How to access the server under DHCP environment

Once DHCP is enabled, there is no way for the user to know which IP is assigned to the server from the server web page. Following is guide how to get to know IP address of the server.



Network Configuration : DHCP Client

Static IP ○ DHCP Client ●

DNS 1	168.126.63.1
DNS 2	168.126.63.2

Once DHCP is enabled, there is not other setting to be changed in the network works configuration except DNS info, if required.

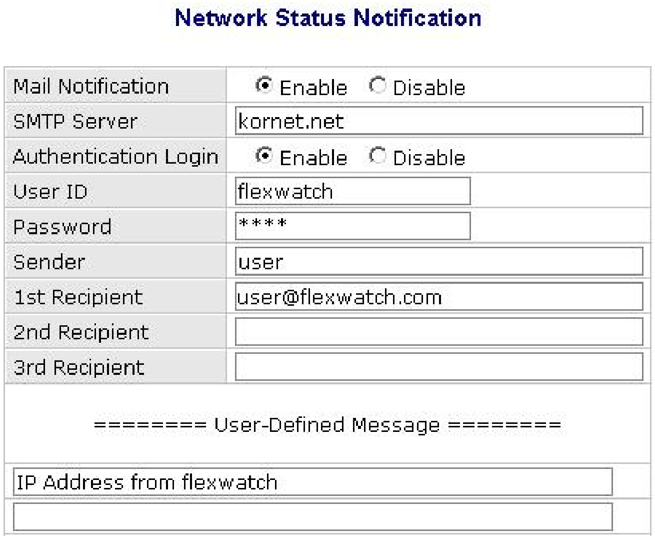
2.1.1.1 IP notification by E-mail service

You can receive IP address of the server through e-mail from the server, when the server is connected to DHCP server. **Please do not enable DHCP client feature till you open a way to receive or get IP address of server.**

1) Check whether you are in the DHCP environment before starting set-up.

2) Go to [**Network Status Notify**] menu in the network configuration mode

3) Set up e-mail account through which you would like to get IP address information when the server is set up DHCP Client.



Network Status Notification

Mail Notification	● Enable ○ Disable
SMTP Server	kornet.net
Authentication Login	● Enable ○ Disable
User ID	flexwatch
Password	****
Sender	user
1st Recipient	user@flexwatch.com
2nd Recipient	
3rd Recipient	

======== User-Defined Message ========

IP Address from flexwatch

4) Now go to Network configuration mode and select DHCP option

*** For more information about e-mail configuration, refer chapter for the e-mail**

configuration in Advanced Service

2.1.1.1 Server access through AOIP server

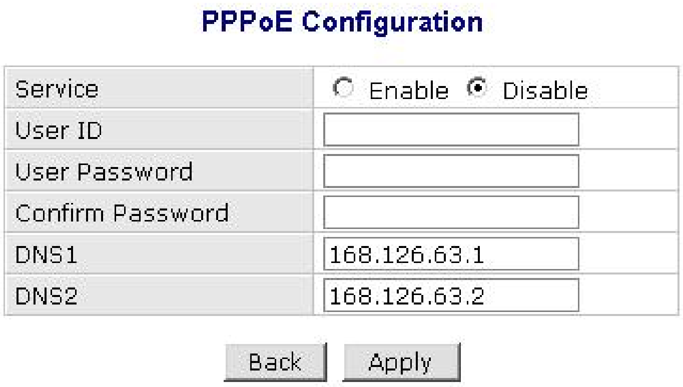
Once Server is registered in the AOIP server and DHCP is enabled, you can access the server through AOIP server. IP address of server can be found from AOIP server as well. In this case you do not need to configure e-mail address setting to get IP address from the server.

Please contact your local vendor or manufacture to get more information about AOIP server which is an IP gateway for Dynamic IP user.

2 PPPoE Configuration

Some DSL or Cable Modem based ISP provides PPPoE based internet connection service. If FlexWATCH™ server must directly be connected to the external DSL or Cable modem, PPPoE option must be enabled.

Note that you must open a way to get IP address information, since there is no way you can get to know IP address of the server through web browser when the server is set to PPPoE network. The only way you can get IP address is through e-mail or AOIP server. Please refer to above DHCP client part to set up e-mail and AOIP connection.



PPPoE Configuration

Service	○ Enable ● Disable
User ID	
User Password	
Confirm Password	
DNS1	168.126.63.1
DNS2	168.126.63.2

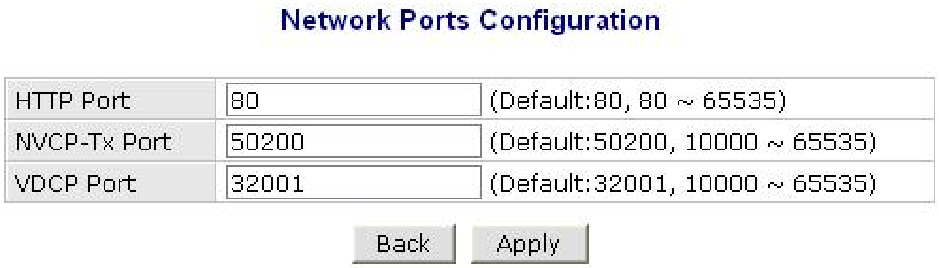
Please contact your local ISP to get User ID and Password for your Internet connection.

☞ **Note**

Once PPPoE is enabled, LAN network setting will be disabled.

3 Network port configuration

HTTP port, NVCP and VDCP ports are application port through which video and audio data can be transmitted over the TCP/IP network.



Network Ports Configuration

HTTP Port	80	(Default:80, 80 ~ 65535)
NVCP-Tx Port	50200	(Default:50200, 10000 ~ 65535)
VDCP Port	32001	(Default:32001, 10000 ~ 65535)

3.1 HTTP port configuration

When you need to change **Default HTTP Port (#80)** to other port, you can change HTTP port. This is very useful when more than one server should be installed behind a router.

By assigning different HTTP port number for each server and configure port-forwarding feature of Router, you can install more than one server behind the router.

For more information about this, please contact your local vendor.

3.2 NVCP –Tx Port

Tx port is a TCP port number through which FlexWATCH^{TM} server can communicate with other devices such as FW-5440 or FW-5000 NDVR servers. This port number is user definable.

NVCP-Tx port must be opened when the FlexWATCH^{TM} server transmits data through Internet in a Passive way (When TX Module Registration is configured as PASSIVE MODE). When NVCP port is to be used, you must open TCP port in the router as well.

3.3 VDCP Port configuration

VDCP port is UDP port for Voice Communication. By changing VDCP port (Default number is 32001), **you can install more than one Voice kit and Video server under the router**.

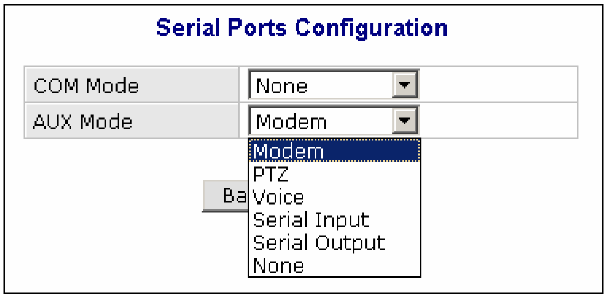
Note that when Voice Kit is connected to Internet, respective UDP port of the router must be opened.

4 WAN Configuration and Application

Server is designed to make a call to ISP or can receive a call from outside so that server can establish Internet connect to send FTP, e-mail or send video & data through PSTN line or other medium. This is best alternative when the broadband Internet access is not available.

4.1 External Modem connection

Modem has to be connected to **AUX Port** with RS-232 Serial Cable.



Serial Ports Configuration

COM Mode	None
AUX Mode	Modem

1) Connect your MODEM and AUX Port at FlexWATCH™ server with RS-232 Serial cable.

2) Go to **Admin Menu** >> **System Configuration** >> **Serial Ports Configuration**

3) Select '**Modem**' at AUX mode and click 'Apply' button.

4) System reboot will be recommended, then click 'Reboot' button.

4.2 Application with Dial-in/out feature

4.2.1 Application with Dial-in

Dial-in is to allow server connection from remote client. This option is useful for the user to connect the server at any time. Especially when the server sends e-mail notification for the alarm and user want to check the situation.

4.2.2 Application with Dial-out

Server can establish the Internet connection through PSTN line and send FTP or e-mail when the alarm condition is triggered by any event.

Following can be done through Dial-out function

- **Pre / post alarm image sending through e-mail**
- **Pre / post alarm image sending to FTP server through FTP function**
- **Establish connection with AOIP server :**

when the event is happened, server can send e-mail notification for the alarm and can keep the connection with AOIP server, not terminating the connection with ISP.
Thus, you can quickly connect the server through AOIP server and view live video. **The key benefit** of using AOIP connection is to view live video without making a separate call to FlexWATCH^{TM} server whenever there is alarm and you can easily access the server. If you are running FW-Manager software, live video will be automatically display on the FW-manager screen when there is any alarm.

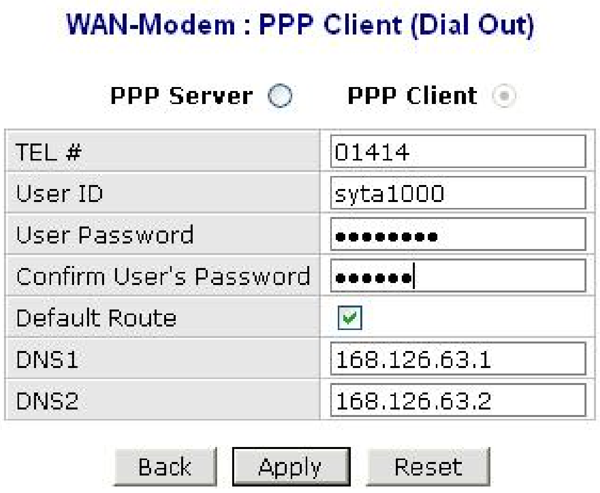
4.3 Dial Out configuration

This is to set up the system to make a call to ISP when the dial out condition is activated to transmit live video or send e-mail or FTP image.

4.3.1 Dial-up through Standard modem

Dial-out through standard PSTN modem is quite common and general.

1) Connect the server to PSTN line through RS-232 cable. Connect the cable to COM Port or server. Use the standard D-Sub 9pin connector provided by PSTN modem.
2) Go to **[WAN (PPP, Modem, etc)]** menu in the Network configuration mode
3) Select "**PPP client**" option and fill out the option field.



WAN-Modem : PPP Client (Dial Out)

PPP Server ○ PPP Client ●

TEL #	01414
User ID	syta1000
User Password	●●●●●●●●●
Confirm User's Password	●●●●●●
Default Route	☑
DNS1	168.126.63.1
DNS2	168.126.63.2

PPP Client :

This means that FlexWATCH^{TM} server act as client and call out to ISP.\

PPP Server :

This means that FlexWATCH^{TM} server acts as a Server and receives a call from remote user.

Tel#, User ID and User password :

ISP phone number and user account for Internet connection to ISP.

Default Route :

Enable this option. When Dial-out option is selected.

Note

If you use **external modem, we recommend** '**3COM U.S.Robotics 56K**' external modem for better performance, although FlexWATCH^{TM} server is designed to flexibly work with different external modem from different manufacturer. If you are to use different external modem from different manufacturer, we recommend you to contact your distributor or contact sales@flexwatch.com to choose compatible modem.

4.3.2 Dial-Out through Media specific device

Dial-out can be done through specific media which is not standard PSTN such as CDMA modem, GSM or GPRS Modem or any type of wireless modem.

This mode is not for general users. Thus, if you need to connect special modem device, please contact your vendor or manufacturer for more information, sales@flexwatch.com

4.4 Dial-in Configuration

Dial-in is to allow client PC to call into the server and get live video through PSTN line. Overall configuration is very similar to that of Dial-out configuration. But much more simple than Dial-out.

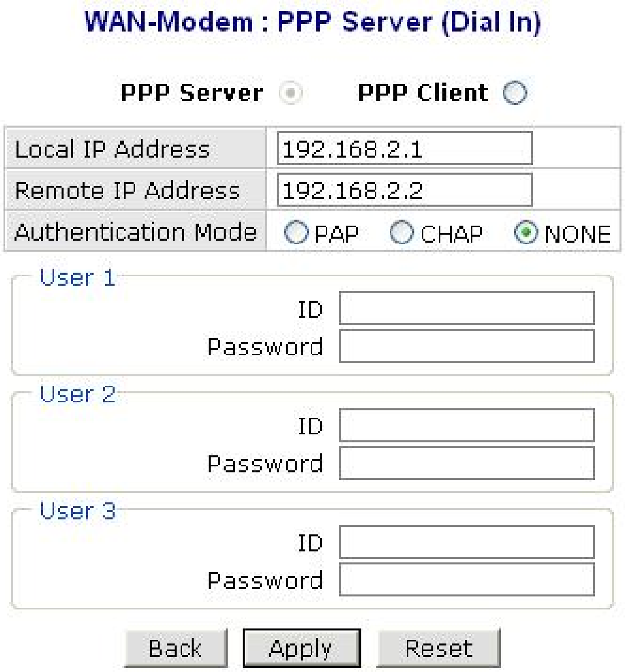
1) Go to **[WAN (PPP, Modem, etc)]** menu in the Network configuration mode.

2) Select "PPP Server". This is to authenticate incoming call to server from remote client.

3) Check Authenticate more as none.

4) Configure User ID and Password, if you need to set up authenticate mode

5) Click [Apply] button and quit configuration menu.



WAN-Modem : PPP Server (Dial In)

PPP Server ● PPP Client ○

Local IP Address	192.168.2.1
Remote IP Address	192.168.2.2
Authentication Mode	○ PAP ○ CHAP ● NONE

Local IP address and Remote IP address

When remote client is connected to the server through modem connection, physical line connection will be done. But no way to view live video unless client runs the web browser of the FlexWATCH^{TM} server.

Local IP address and Remote IP address is virtual IP address which is used at the time of Modem connection only

Local IP address :

System default IP address **(192.168.2.1)** resides in the FlexWATCH^{TM} server for **modem connection** only. So when you connect the FlexWATCH^{TM} server from remote PC using dial-up networking and physical connection is made, you need to run your web browser and enter this system default IP address**(192.168.2.1)** to view live video. You can change this system default IP address as well. But it is recommended not to change system default IP address for modem connection to prevent any possible error.

Remote IP address :

IP address which is automatically given to remote client PC by FlexWATCH^{TM} server when FlexWATCH^{TM} server is connected by remote client PC using dial-up networking. This IP address (**192.168.2.2**) is for data communication between FlexWATCH^{TM} server and Remote client PC. So **you do not need to change this IP address**. But if you change default IP address of FlexWATCH^{TM} server (**192.168.2.1**) for modem connection to different class of IP address, you need to change remote IP address to the same class of IP to match the IP class.

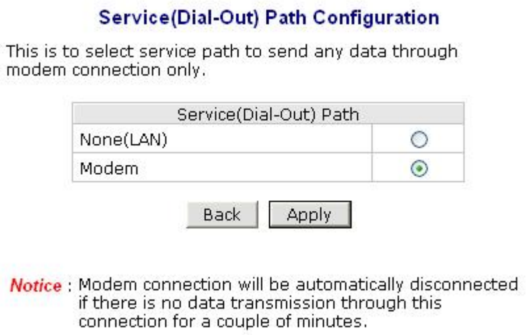
☞ ***Note that when Local IP address is change, remote IP address should be changed into the same class of the IP address.***

5 Service Path

This is to specify service path through which server can send any information to target device.

1) Go to Service path menu in the service configuration mode

2) Select "**Modem**", if any data should be sent through PSTN or external modem device and click "**Apply**" button.



Service(Dial-Out) Path Configuration

This is to select service path to send any data through modem connection only.

Service(Dial-Out) Path	
None(LAN)	○
Modem	●

Notice : Modem connection will be automatically disconnected if there is no data transmission through this connection for a couple of minutes.

LAN : This is default path the send any data to outside.

Modem : when PSTN or other medium than LAN is used to send data to outside. This service port must be checked when any data is to be sent through PSTN or other medium than LAN which is connected to COM port.

Note

Service path must be set up and checked before starting WAN configuration to send any data through external PSTN modem connection or equivalent

If LAN is to be used, select "None(LAN)" option.

6 AOIP Setup

AOIP (Always-On-IP) is an IP gateway through which user can access the FlexWATCH™ server when it is connected to Dynamic IP address. Thus, if the server should be connected to the Dynamic IP network and you want to view live video from anywhere, it is the right solution for you.

6.1 How to use AOIP service

Following is a step you need to take to use AOIP service

- Contact your local vendor or sales@flexwatch.com to get user account for AOIP service.
- Register product in the AOIP server under your account
- Set up your network (Port mapping function of your router)
- Enable AOIP service option in the FlexWATCH™ server.

- Once things are set up, you can login to AOIP server and connect your FlexWATCH™ server.

☞ ***Note***

AOIP is proprietary data service run by FlexWATCH™ or its business partners around the world. Thus, depending on the country AOIP service can run by your local vendor or master distributor or in some case, you need to user AOIP server run by manufacturer.

More detailed information about how to use can be acquired by contact your local distributor or sales@flexwatch.com .

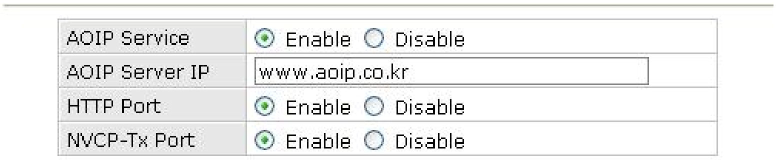
6.2 AOIP configuration

As described above, once you register product in the AOIP server and Network setting is correctly done to user AOIP function, you need to configure AOIP function in the FlexWATCH™ server.

1) Check the "**Enable**" option to use AOIP function

2) Type in AOIP server address. Either Domain name or IP address can be typed in.

3) Select whether to use HTTP or NVCP-TX port. HTTP port must be selected to view



AOIP Service	● Enable ○ Disable
AOIP Server IP	www.aoip.co.kr
HTTP Port	● Enable ○ Disable
NVCP-Tx Port	● Enable ○ Disable

AOIP Server IP :

AOIP server IP is subject to change depending on where you are and who is your local distributor, since AOIP server can be run by local distributor in some countries. If there is no local AOIP service available, you can contact manufacturer to use. www.aoip.co.kr is AOIP Service address run by manufacturer.

HTTP Port:

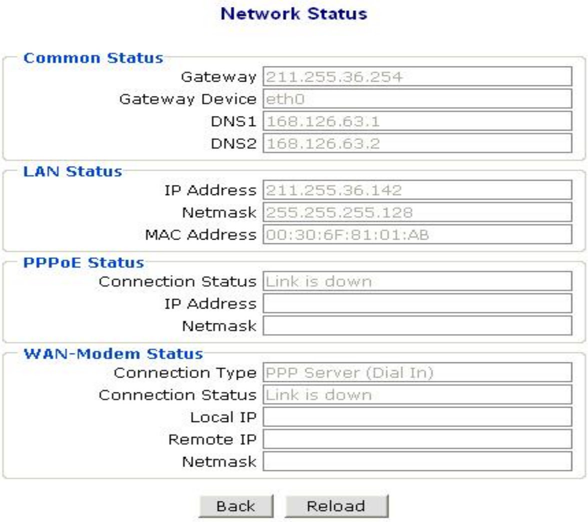
This is enable HTTP connects to AOIP server. You must select "Enable" option.

NVCP-TX Port:

NVCP-Tx Port should be enabled only when video is transmitter to NDVR server such as FW-5440 and FW-5000, or Video proxy server supplied by FlexWATCH^{TM} server. If not, do not enable this option.

7 Network Status

You can see all the network status configured in the system through "**Network st**atus" option. Please Select "Network Status" menu in the Network configuration mode of Admin Window.



Network Status

Common Status

Gateway 211.255.36.254
Gateway Device eth0
DNS1 168.126.63.1
DNS2 168.126.63.2

LAN Status

IP Address 211.255.36.142
Netmask 255.255.255.128
MAC Address 00:30:6F:81:01:AB

PPPoE Status

Connection Status Link is down
IP Address
Netmask

WAN-Modem Status

Connection Type PPP Server (Dial In)
Connection Status Link is down
Local IP
Remote IP
Netmask

External Device connection & configuration

External device such as Serial input device, Serial output (UART) device, PTZ (pan/Tilt/Zoom) device, Audio kit and Alarm input and output device can be connected to the system and controlled over the TCP/IP network.

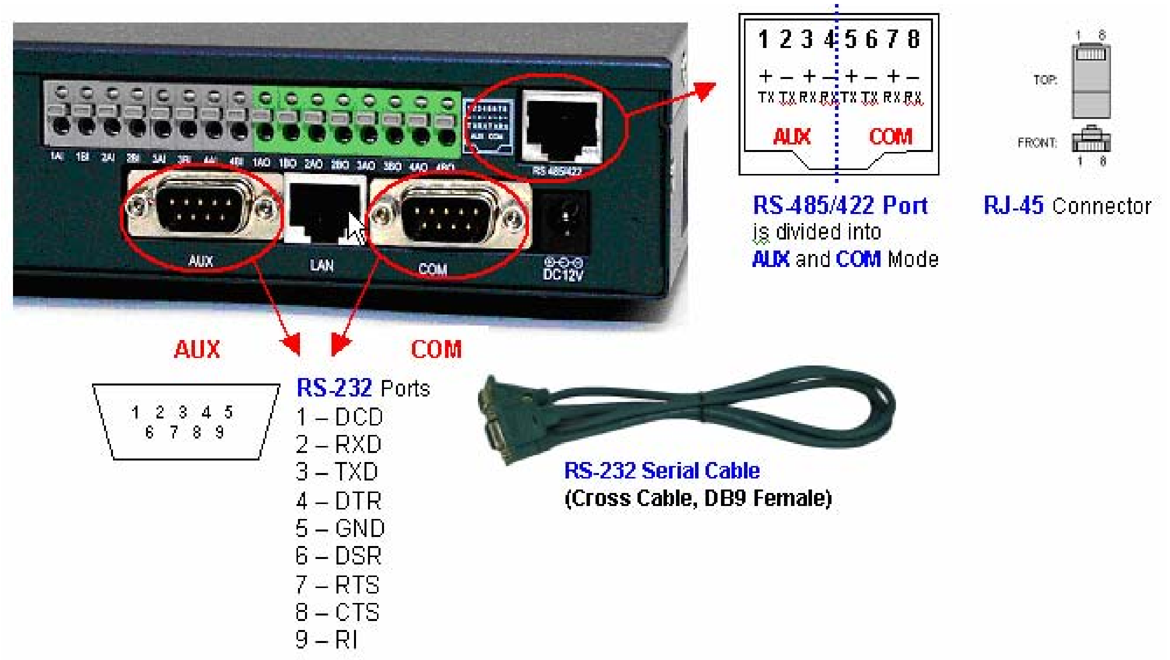
1 Serial Ports Configuration Guide

This chapter will guide you how to install and configure Serial-interface devices. FlexWATCH™ server is designed to support simultaneously **TWO different Serial-interface devices (RS-232, RS-485, RS-422)** through **COM** and **AUX** ports.

1.1 Hardware Description

There are two DB-9 terminal ports (**Aux and COM**) for RS-232 interfaces, and one RJ-45 terminal port for RS-485 and RS-422 interfaces at the rear part of FlexWATCH™ server as below picture. RJ-45 terminal port provides 8 pins that are divided into **AUX and COM** part as well.

1.1.1 Pin-Out Information

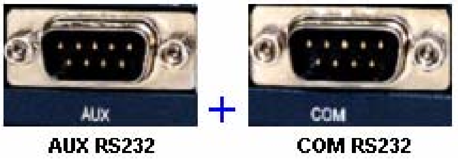
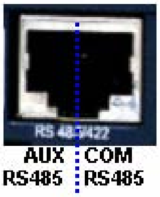
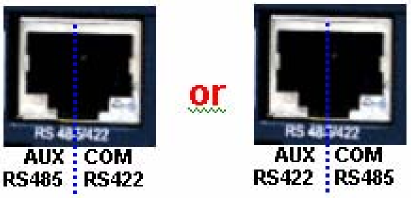
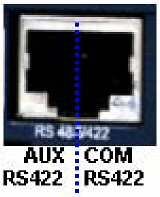

1 2 3 4 5 6 7 8
+ – + – + – + –
TX TX RX RX TX TX RX RX
AUX
COM
RS-485/422 Port
is divided into
AUX and COM Mode
TOP
FRONT
1 8
RJ-45 Connector
AUX
LAN
COM
DC12V
AUX
COM
1 2 3 4 5
6 7 8 9
RS-232 Ports
1 – DCD
2 – RXD
3 – TXD
4 – DTR
5 – GND
6 – DSR
7 – RTS
8 – CTS
9 – RI
RS-232 Serial Cable
(Cross Cable, DB9 Female)

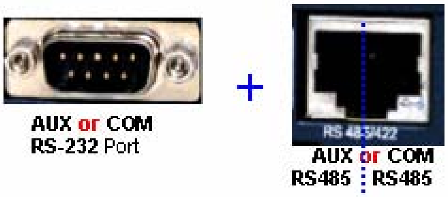
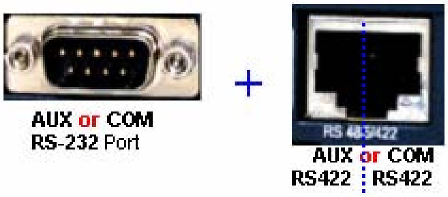
Available Devices	**COM**	**AUX**
Console (Hyper Terminal)	O	X
Modem	X	O
PTZ	O	O
Voice	O	O
Serial Input	O	O
Serial Output	O	O
None	O	O

1.1.2 Ports Connection for using two different devices.

AUX and COM part is provided for RS-232 and RS-485 or RS-422 connection. This enables user to connect more external devices to the server and selectively use them per his needs.

But **same type of port for RS-232, RS-485 or RS-422 can not simultaneously be used**. For example, if COM part of RS-232 is used by Hyper Terminal Connection, COM part of RS-485 can not be operative. In this case, AUX part of RS-485/RS-422 or RS-232 port should be used.

Interface combination	**Ports Connection**
RS-232 + RS-232	 AUX + COM AUX RS232 COM RS232
RS-485 + RS-485	 RS 485/422 AUX COM RS485 RS485
RS-485 + RS-422	 RS 485/422 AUX COM RS485 RS422 or RS 485/422 AUX COM RS422 RS485
RS-422 + RS-422	 RS 485/422 AUX COM RS422 RS422

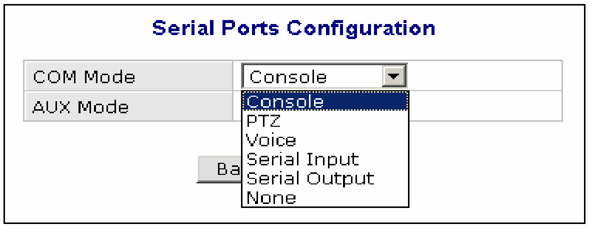
RS-232 + RS-485	 AUX or COM RS-232 Port + RS 485/422 AUX or COM RS485 ⋮ RS485 AUX(RS232) and COM(RS485) or COM(RS232) and AUX(RS485)
RS-232 + RS-422	 AUX or COM RS-232 Port + RS 485/422 AUX or COM RS422 ⋮ RS422 AUX(RS232) and COM(RS422) or COM(RS232) and AUX(RS422)

☞ ***You cannot make use of AUX (RS232) port and AUX (RS485, 422) part at the same time. Also it is not available to use of COM (RS232) port and COM (RS485, 422) part together.***

2 Installation & Configuration of External Device

2.1 Console(Hyper Terminal cable connection)

Console **has to be connected to COM Port with RS-232** Serial cable.



Serial Ports Configuration

COM Mode: Console

AUX Mode

Console
PTZ
Voice
Serial Input
Serial Output
None
Ba

1) Connect COM1 or COM 2 Port at your PC and COM Port at FlexWATCH™ server with RS-232 Serial cable.

2) Go to Admin Menu >> System Configuration >> Serial Ports Configuration

3) Select '**Console**' at COM mode, and Click 'Apply' button

4) System reboot will be recommended, then click 'Reboot' button.

2.2 Serial Input device

Serial input device such as Car Speed sensor, BOG sensor, POS (Point of sales), ATM device which communicate with external device through RS-232 port can be integrated with the system. And that data can be transmitted along with video to anywhere over the TCP/IP network.

1) Connect your Serial Input Device to **RS422/485 Port or RS232 (COM or AUX) port**.

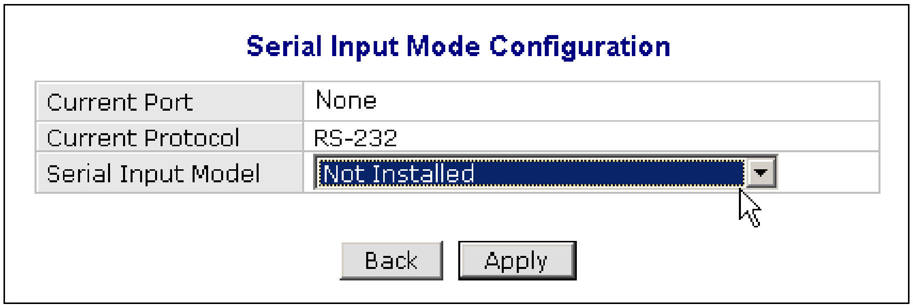
2) Go to Admin Menu >> System Configuration >> Serial Ports Configuration

3) Select 'Serial Input' at COM or AUX mode, and Click 'Apply' button.

4) System reboot will be recommended, then click 'Reboot' button.

5) After rebooting, Go to Admin Menu >> System Configuration >> Serial Ports Configuration

6) Click "**Serial Input Mode**", then following window will show up.



Serial Input Mode Configuration

Current Port	None
Current Protocol	RS-232
Serial Input Model	Not Installed

7) Select the installed Serial Input Device Model on the dropdown menu as above.

8) Click 'Apply' button.

☞ ***Note***

Serial Input device protocol can separately be uploaded into the system per customer needs. User can upload serial input device protocol file which is provided by manufacturer only.

This function is not for general use. Thus, if you need more close information about this, please contact your local distributor or manufacturer for further information, sales@flexwatch.com.

2.3 Serial output device

The system supports to relay third party command to target device through Serial output device control mode. Through this, user defined message can be reached to target device

The system supports two different modes. One is X10 protocol for PLC (Power Line Communication) and UART(Universal Asynchronous Receiver Transmitter) device.

2.3.1 Serial Output Configuration

Following is guide for hardware cabling and setting.

1) Connect your Serial Output Device to **RS422/485 Port or RS232 (COM or AUX) port**.

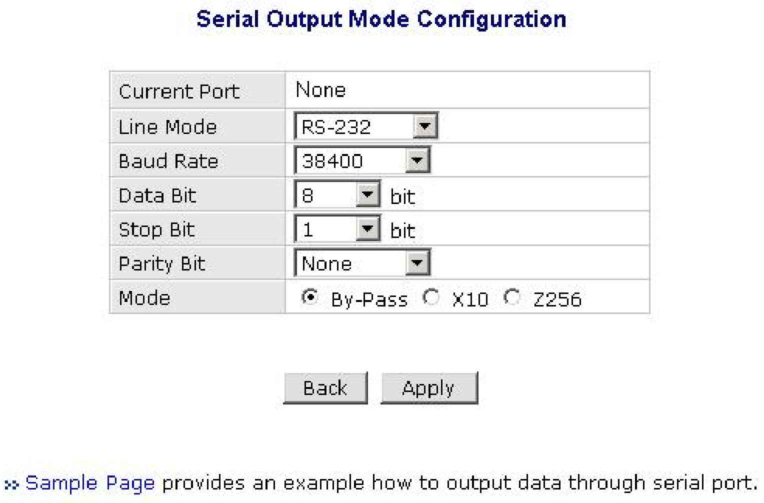
2) Go to Admin Menu >> System Configuration >> Serial Ports Configuration.

3) Select 'Serial Output' at COM or AUX mode, and Click 'Apply' button.

4) System reboot will be recommended, then click 'Reboot' button.

5) After rebooting, Go to Admin Menu >> System Configuration >> Serial Ports Configuration.

6) Click "**Serial Output Mode**", then following window will show up.



Serial Output Mode Configuration

Current Port	None
Line Mode	RS-232
Baud Rate	38400
Data Bit	8 bit
Stop Bit	1 bit
Parity Bit	None
Mode	● By-Pass ○ X10 ○ Z256

» Sample Page provides an example how to output data through serial port.

G. After setting up the parameters in the each filed, click '**Apply**' button. **Note that if you are using X10 device protocol, you do not need to set up parameters, but simple select X10 "Enable" option.**

2.3.2 X 10 device & Z256

X10 and Z256 is a protocol name of Device which is to control electronic devices over the Power line communications. Using this control mode, you can build up a system to control any electronic device over the TCP/IP network through FlexWATCH^{TM} server
This function is highly recommended for Home automation or remote device control application.

This function is not for general use. Thus, if you need more se information about this, please contact your local distributor or manufacturer for further information, sales@flexwatch.com.

2.3.3 UART(Universal Asynchronous Receiver Transmitter) device

By-pass command mode is supported by the system so that user can send command string to target device through the server from the remote area.
By-pass command string can be sent either by third party application program or control panel inside of the system.

A. By-pass command string from third party

This is to send command string from third party application program to the target device connected to the server. More about this function can be supplied by HTTP CGI API guide.

B. Control panel inside of the system

You can create control panel of external device inside of the server and control target device through server web page.

This function is not for general use. Thus, if you need more information about this, please contact your local distributor or manufacturer for further information, sales@flexwatch.com.

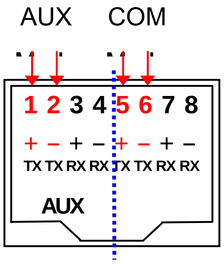
2.4 PTZ device connection and configuration

PTZ(Pan/Tilt/Zoom) device connected to the server can be controlled through either standard web browser or specific application program over IP network.

2.4.1 PTZ connection

When you install a RS-485/422 interfaced PTZ model:

PTZ device has to be connected to **RS422/485 Port** with RJ-45 connector. And it can be configured either in **AUX** or **COM** part. As mentioned above please check whether AUX or COM port for RS-232 is already assigned or not and use different part for RS-422/RS-485 connection which is not assigned by RS-232 Port.



When you select PTZ at **AUX part**,
make use of **Pin No. 1 and 2** from RS422/485 port.
When you select PTZ at **COM part**,
make use of **Pin No. 5 and 6** from RS422/485 port.

When you install a RS-232 interfaced PTZ model:

PTZ device has to be connected to **AUX** or **COM Port** with RS-232 Serial Cable. Standard RS-232 cable can be used to connect AUX or COM port.

1) Connect your PTZ device into **RS232** (COM or AUX) port as above explanation.

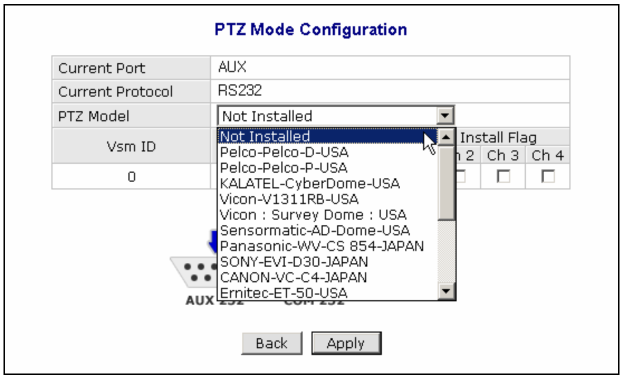
2) Go to Admin Menu >> System Configuration >> **Serial Ports Configuration**.

3) Select 'PTZ' at COM or AUX mode, and click 'Apply' button.

4) System reboot will be recommended, then click 'Reboot' button.

5) After rebooting, Go to Admin Menu >> System Configuration >> Serial Ports Configuration.

6) Click "PTZ Mode", then following window will show up



PTZ Mode Configuration

Current Port	AUX
Current Protocol	RS232
PTZ Model	Not Installed

Not Installed
Pelco-Pelco-D-USA
Pelco-Pelco-P-USA
KALATEL-CyberDome-USA
Vicon-V1311RB-USA
Vicon : Survey Dome : USA
Sensormatic-AD-Dome-USA
Panasonic-WV-CS 854-JAPAN
SONY-EVI-D30-JAPAN
CANON-VC-C4-JAPAN
Ernitec-ET-50-USA
Vsm ID
0
Install Flag
Ch 3
Ch 4
AUX
Back
Apply

7) Select the installed PTZ Model on the dropdown menu as above.

8) Select the Channel number installed with the PTZ, and click 'Apply' button

2.4.2 Supported PTZ(Pan/Tilt/Zoom) Device list

- Following is list of PTZ devices which are directly supported by FlexWATCH^{TM} server. Note that some of PTZ has not been field approved, although manufacturer integrated its protocol into FlexWATCH^{TM} server. Thus, it is highly recommended for you to use only field approved PTZ device.
- In addition, although Manufacturer integrated Protocol of PTZ device and did field test, PTZ can not be workable, since PTZ manufacturer can change its protocol or other functions. Thus, it is highly recommended for you to contact your distributor or sales@flexwatch.com to make sure its connectivity through FlexWATCH^{TM} server.
- You are also required to refer to Technical note for **installation guide** per respective PTZ device in the CD manual.

Supported PTZ List by FlexWATCH^{TM} Server

Supplier	Model	Command	Preset	Auto PAN	Program Only	Lab Test	Field Test
** Pelco	Spectra	485 (P)	O			O	O
** Pelco	Spectra	485(D)	O			O	O
* Panasonic	WV-CS854	485		O			O
** AD	Delta Dome	485		O		O	O
* Samsung Techwin	SPD1600	485	O	O			O
* Samsung	SCC-641	485	O	O		O	O
Seyeon	FSD-230	485	O				O
Seyeon	SPT-101(2)	485		O			O
Seyeon	SRX-500	485	O	O			O
CANON	VC-C4	232	O	O		O	O
* VICON	V-1311	485	O	O			O
***VICON	Surveyor	485	O				O
KALATEL	Cyber	232	O	O		O	
SONY	EVI-D30	232					O
Samsung	MRX-1000	485		O		O	O
***Honeywell	HSDN-251	485	O	O			O
InterM	VRX-2201	485		O		O	
NIKO	NK97-CHE	485	O	O			O
ELMO	ELDOME	485	O	O			O
ERNITEC	BDR-510	485	O	O		O	

RNK	RNK-DOME	485		O			O
DAIWA	DMP-23-H1	485	O	O			O
LILIN	PIH-717	485				O	
PHILIPS	Auto Dome	485					O
FINE system	CRR-1600I	232		O		O	O
Samsung Techwin	SRX-100B	485		O		O	O

NOTE : Symbol Reference

* : Preset function was program only.

** : Preset function was Lap Tested only.

*** : Preset function was field Tested

2.5 Voice Kit Connection and configuration

G.723.1 which is international standard for VOIP (Voice Over IP) communication based FW-V10s voice kit can work with FlexWATCH™ server and you can enjoy not only live video stream but also full duplex two real time Voice through web browser or proprietary application program.

Voice broadcasting for voice connection by multiple users is also supported by the system as well.

Note

Once Multi user connection is enabled, only root Account user can enjoy full duplex audio and rest of users can listen only.

1) Connect **RS-232 Serial Cable with FW-V10S to AUX or COM port** of FlexWATCH™ server. Serial cable is provided with FW-V10S . Refer to PIN out diagram above.

2) Connect RS-232 Serial Cable to FW-V10S.

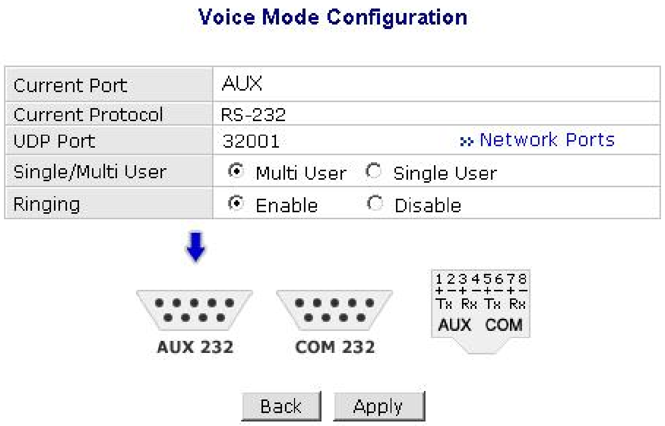
3) Go to Admin Menu >> System Configuration >> Serial Ports Configuration.

4) Select '**Voice**' at COM or AUX mode, and click 'Apply' button. Please note that Voice kit can be connected **either AUX or COM port (through RS-232) only**.

5) System reboot will be recommended, then click 'Reboot' button.

6) After rebooting, Go to Admin Menu >> System Configuration >> Serial Ports Configuration

7) Click "Voice Mode", then following window will show up



Voice Mode Configuration

Current Port	AUX
Current Protocol	RS-232
UDP Port	32001 :: Network Ports
Single/Multi User	● Multi User ○ Single User
Ringing	● Enable ○ Disable

UDP Port :

Voice kit use UDP port to transmit Voice kit. If voice communication should be done through WAN network, please make sure **UDP port is not blocked to Internet connection in router or firewall etc**.

The default VDCP (Voice Device Control Protocol) port is 32001, please go to Network port configuration mode to change VDCP port if required.

Application Idea

By changing VDCP port, you can install multiple Voice kit and FlexWATCH^{TM} server behind the single broadband network.

Single / Multi User:

Once Multiple users are selected, only **Admin account user can enjoy full duplex Audio** and **User account user can listen only**.

Ringing :

This is to enable or disable sounds from the internal speaker of voice kit when there is a connection to Voice kit from outside.

8) Click "Save" button to save your configuration.

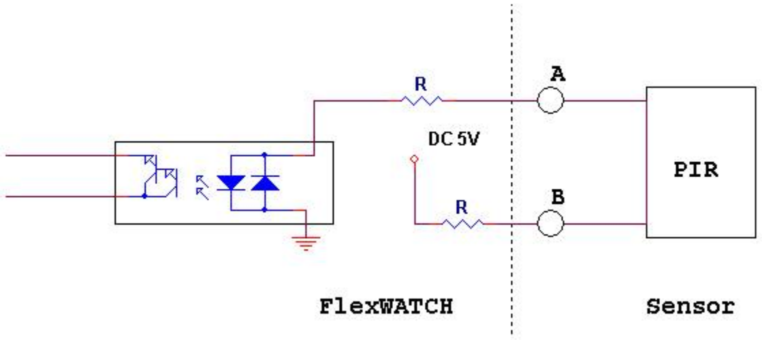
3 Alarm input device connection

FlexWATCH^{TM} server has Alarm Sensor interface so that it can send alarm notification by activating e-mail or FTP function or activate alarm output device such as Siren or light.

FlexWATCH^{TM} server supports opto-coupled input circuit and any dry contact type of Alarm sensor can easily be interfaced to the server.

Following is circuit diagram for Alarm input part.

Opto-coupled Sensor input Diagram



1) Simply connect the alarm sensor to the server.
2) Go to "Alarm input/out" menu to name the alarm input name.
3) Once configuration is done, alarm based services can be done such as e-mail, FTP, Sensor notification

Application Idea

Followings are list of services which is related to alarm input device connection. Thus, when you use following features, you must make sure that Alarm input device is correctly configured.

- e-mail, FTP, Sensor notification, Alarm output device control.

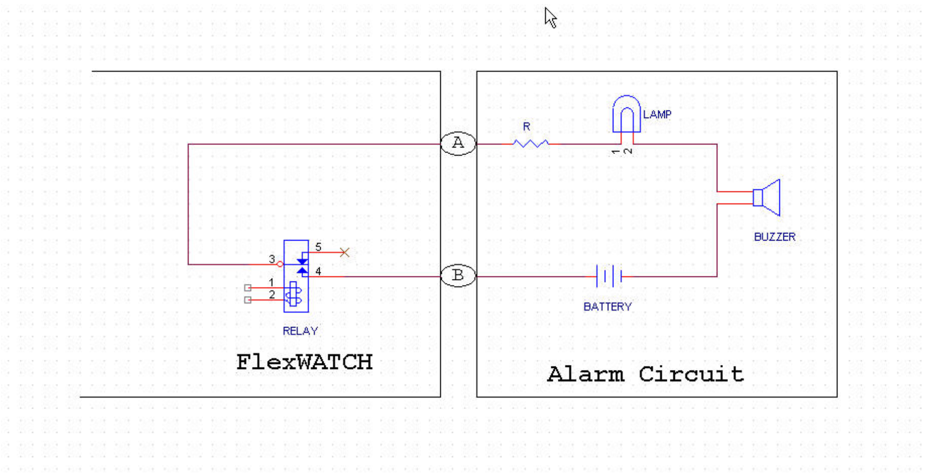
4 Alarm Output(Relay output) device connection

FlexWATCH^{TM} server can easily be interfaced with Alarm output device such as Siren and light. Manual or automatic control of alarm output device is supported by the server so that relay output device such as siren, light or any output device can remotely be controlled through standard web browser or third party application program.

4.1 Alarm output device connection

Any Relay contact type of output device can be interfaced with FlexWATCH™ server. Simple connect the Alarm output device to Relay output(DO) port of FlexWATCH™ server. Following is a circuit diagram for alarm output terminal.

Relay Output Circuit Diagram



4.2 Manual control of Alarm output device

Alarm output device can manually be controlled through simple viewer page or admin page.

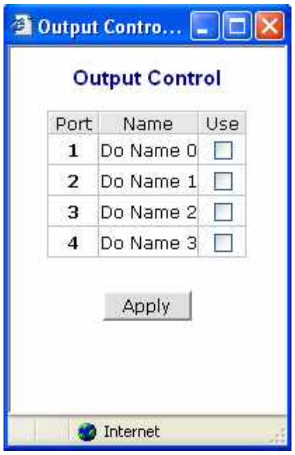
4.2.1 Alarm output device through web browser

Alarm output device control panel can separately run in the simple viewer page, if control authority for Alarm output device is given to user. If not allow, alarm output device control panel will not be loaded in the simple viewer page.

1) Go to simple viewer web page

2) Click "**Output control**" button in the web page

3) Check the output port number and click apply button to activate the alarm output device



Output Control

Port	Name	Use
1	Do Name 0	☐
2	Do Name 1	☐
3	Do Name 2	☐
4	Do Name 3	☐

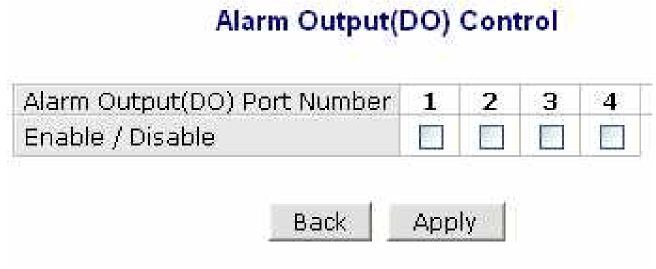
4.2.2 Alarm output device through Admin Page

Alarm output device can manually be controlled through Admin page of the system. This option is recommended when web browser based alarm output control panel is hided and administrator want to manually control Alarm output device.

1) Run Admin configuration panel

2) Click Alarm output control option in the Service configuration mode

3) Check the alarm output port and click "Apply" button



Alarm Output(DO) Control

Alarm Output(DO) Port Number	1	2	3	4
Enable / Disable	☐	☐	☐	☐

4.3 Automatic Control of Alarm Output device

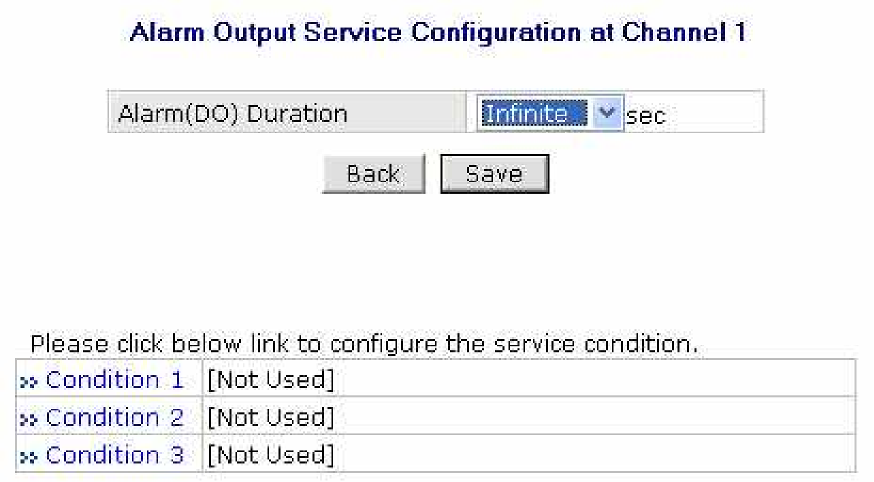
Alarm Output device can automatically be controlled by setting up control condition properly. This is to automatically to activate alarm output or any relay output device connected to the server.

Up to three different conditions per alarm output port with schedule, Sensor or its combination is provided so as to set up powerful and various working condition for each alarm output device.

1) Go to Advance service option in the Service configuration mode in the Admin window.

2) Click None buffering service menu and select "Alarm output" menu.

3) Check the service "Enable" option and select output port



Alarm Output Service Configuration at Channel 1

Alarm(DO) Duration: Infinite sec

Please click below link to configure the service condition.

» Condition 1	[Not Used]
» Condition 2	[Not Used]
» Condition 3	[Not Used]

4) Select Alarm Duration time from the drop down menu.

Note Alarm Duration time is to set up Alarm active time when alarm output device is activated by any condition.

5) Go to Condition mode and set up condition to activate Alarm output device.

Advanced Service configuration

Advanced service configuration is intended to provide more sophisticated functions which are required by sophisticated users. Thus, if you are not familiar with or not good at advanced features, we recommend you to read this guide carefully and consult with your local vendor to get more close information about these features.

Advanced service can be categorized into **Buffering service** and **None buffering service** depending on whether server stores pre/post alarm video in the system memory.

Buffering service means that the server can store pre/post alarm image in the system memory and send stored image through FTP or e-mail or allow user to view stored image inside of memory. With this feature user can get pre/post alarm image through e-mail or FTP without missing any video before and after the event or playback stored Alarm buffered image by connecting the server.

None buffering service means that Advance service will be done without image buffering inside of the memory. FTP(Periodic), Sensor notification service and Alarm output device control can be provided as a none buffering service option.

1 Buffering Service

Following services can be done by image buffering services.

e-mail : Up to 10 frame of Pre/post alarm image can be sent when there is event is occurred.

FTP (Rising or Falling edge) : Up to 256 frames of pre/post alarm image per video channel can be sent to ftp server when the event is occurred.

Alarm buffering service :

Pre configured number of Pre/post alarm image will be stored in the system memory and user can playback stored image through web browser.

Steps to use Buffering service

Following is a step to configure and use Buffering services

A. System memory allocation : This is to allocated limited system memory for e-mail

& ftp and Alarm buffering service

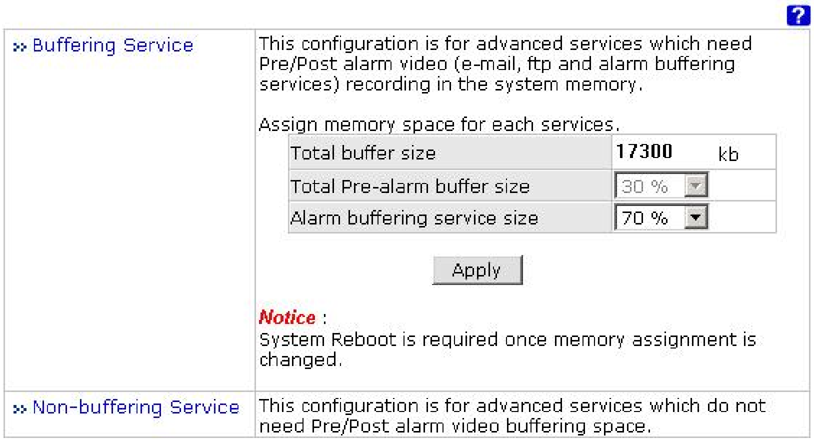
B. Pre alarm buffer size : Once memory allocation is done, assign **Pre alarm buffer size (Pre alarm image buffer pool)** to be used for e-mail, FTP and Alarm buffering services. Any pre alarm buffer for respective e-mail, ftp and Alarm buffering services can be done within Pre alarm buffer size.

C. Pre/Post alarm for respective service : Once Pre Alarm Buffer Size is decided, go to respective e-mail, ftp and alarm buffering service menu and configure the options.

1.1 System and Pre Alarm Buffer memory

1.1.1 System Memory allocation

The number of Pre/Post alarm image for advanced services should be pre-defined to effectively use the limited memory capacity.



»» Buffering Service

This configuration is for advanced services which need Pre/Post alarm video (e-mail, ftp and alarm buffering services) recording in the system memory.

Assign memory space for each services.

Total buffer size	17300	kb
Total Pre-alarm buffer size	30 %	
Alarm buffering service size	70 %	

Notice :
System Reboot is required once memory assignment is changed.

»» Non-buffering Service

This configuration is for advanced services which do not need Pre/Post alarm video buffering space.

Total Buffer size :

This shows the maxim system memory for alarm buffering services.

The number of maximum total buffer frame for respective services can be decided by following formula

Total buffer size / file size = number of total buffer frame

e.g) 500 KB / 10KB = 500 frames which is possible total buffer size.

Total Pre-alarm Buffer size :

This is to assign memory space for the services that Pre Alarm video buffer is required such as e-mail and FTP (Edge service) and Alarm buffering service. Once it is configured, pre alarm buffer size for respective camera can be done within this assigned memory. Note that Pre Alarm buffer for even Alarm buffering service can be done within this memory size.

Thus, you need to be careful to assign memory for this service. The rest of memory after setting up Alarm buffer service memory capacity will be assigned to this service configuration

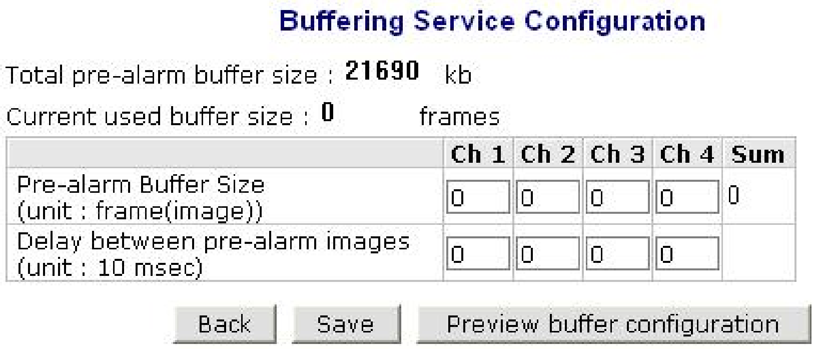
Alarm Buffering Service size :

To assign memory for Alarm buffering service to save pre/post alarm image in the system memory so that user can playback stored video in the system through web browser or download it. Note that **Pre alarm buffer for Alarm buffering service can be done within the Pre-alarm Buffer size**. Thus, you need to count in required pre alarm buffer for alarm buffering service and reserve enough space for this service in the **Pre-alarm Buffer size.**

1.1.2 Pre alarm buffer size

Pre alarm buffer size (Image Buffer Pool) means **the number of images to be stored and continuously refreshed in the system memory**.

Maximum Pre alarm buffer should be the half size of Memory capacity, since Pre alarm images for e-mail, FTP or alarm buffering service are taken from Pre alarm buffer pool and any Pre alarm image for these services require additional memory space.



Buffering Service Configuration

Total pre-alarm buffer size : 21690 kb

Current used buffer size : 0 frames

	Ch 1	Ch 2	Ch 3	Ch 4	Sum
Pre-alarm Buffer Size (unit : frame(image))	0	0	0	0	0
Delay between pre-alarm images (unit : 10 msec)	0	0	0	0	

Pre-alarm Buffer size :

This is to assign pre-alarm image buffer for each camera. Once this is configured, the maximum number of pre alarm for e-mail, ftp or Alarm buffering service (Pre alarm only) can be done with this buffer size, if there is enough memory space for respective services. Note that there must be enough memory space left for e-mail, ftp and Alarm Buffering service (Pre alarm only), since respective service (e-mail, ftp or Alarm buffering service) consumes separate memory in addition to pre alarm buffer size configured to make a real service.

Delay between pre-alarm image :
This is the set up pre alarm speed when the server store image in the system memory. **1000mse is equal to 1sec and basic unit is 10msec**. If you want to get 10fps pre-alarm speed, 10 will be very appropriate number for Delay value.

*** Maximum Pre alarm buffer should be the half size of Total Pre Alarm buffer size memory assigned in the system, since Pre alarm images for e-mail, FTP or alarm buffering service are taken from Pre alarm buffer pool and any Pre alarm image for these services require additional memory space.**

1) Go to Advance service mode in the Service configuration section
2) Go to "**Buffering service**" mode
3) Set up pre-alarm Buffer size and delay time.
4) Click "Buffer Calculator" button to run the calculator.

1.2 Buffer calculator

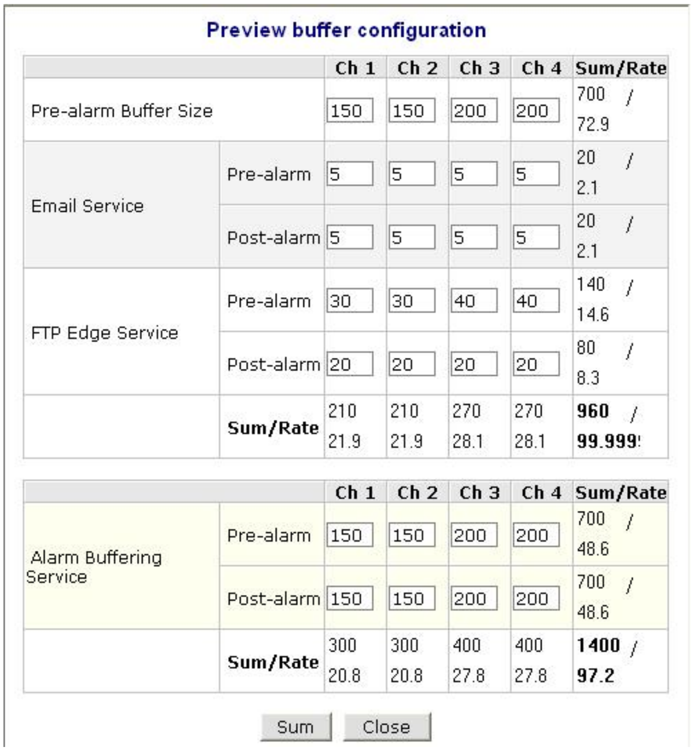
Through "**Buffer Calculator**" option, you can easily calculate assignable pre/post alarm buffer size for each channel before setting up Pre/Post alarm buffer frame in the system memory.

Following is logic for Pre/Post alarm assignment. By running buffer calculator you can try pre/post alarm size.

Total buffer size	**23500 kb**
Total Pre-alarm buffer size	(40%)

Alarm buffering service size	(60%)

- **Total Buffer size is variable depending on the memory used by the system**



Preview buffer configuration

		Ch 1	Ch 2	Ch 3	Ch 4	Sum/Rate
Pre-alarm Buffer Size		150	150	200	200	700 / 72.9
Email Service	Pre-alarm	5	5	5	5	20 / 2.1
	Post-alarm	5	5	5	5	20 / 2.1
FTP Edge Service	Pre-alarm	30	30	40	40	140 / 14.6
	Post-alarm	20	20	20	20	80 / 8.3
	Sum/Rate	210 21.9	210 21.9	270 28.1	270 28.1	**960** / **99.999**

		Ch 1	Ch 2	Ch 3	Ch 4	Sum/Rate
Alarm Buffering Service	Pre-alarm	150	150	200	200	700 / 48.6
	Post-alarm	150	150	200	200	700 / 48.6
	Sum/Rate	300 20.8	300 20.8	400 27.8	400 27.8	**1400** / **97.2**

- **Total number of Pre Alarm+ Post Alarm for FTP per channel < 256 frame.**
- **Total number of Pre + Post alarm for e-mail per channel <10 frames for channel.**
- **Pre alarm frame for FTP & e-Mail and Alarm buffer service shall be done within Total pre-alarm buffer size**
- **Post alarm for FTP & e-mail has nothing to do with Total buffer size.**
- **Post alarm for Alarm buffering service can be done within the Memory allowed by Alarm buffering service size.**
- **The ratio of sum in the Buffer Calculator should be less than 100%.**

1) Go to Advance service mode in the Service configuration section

2) Go to Buffering service mode

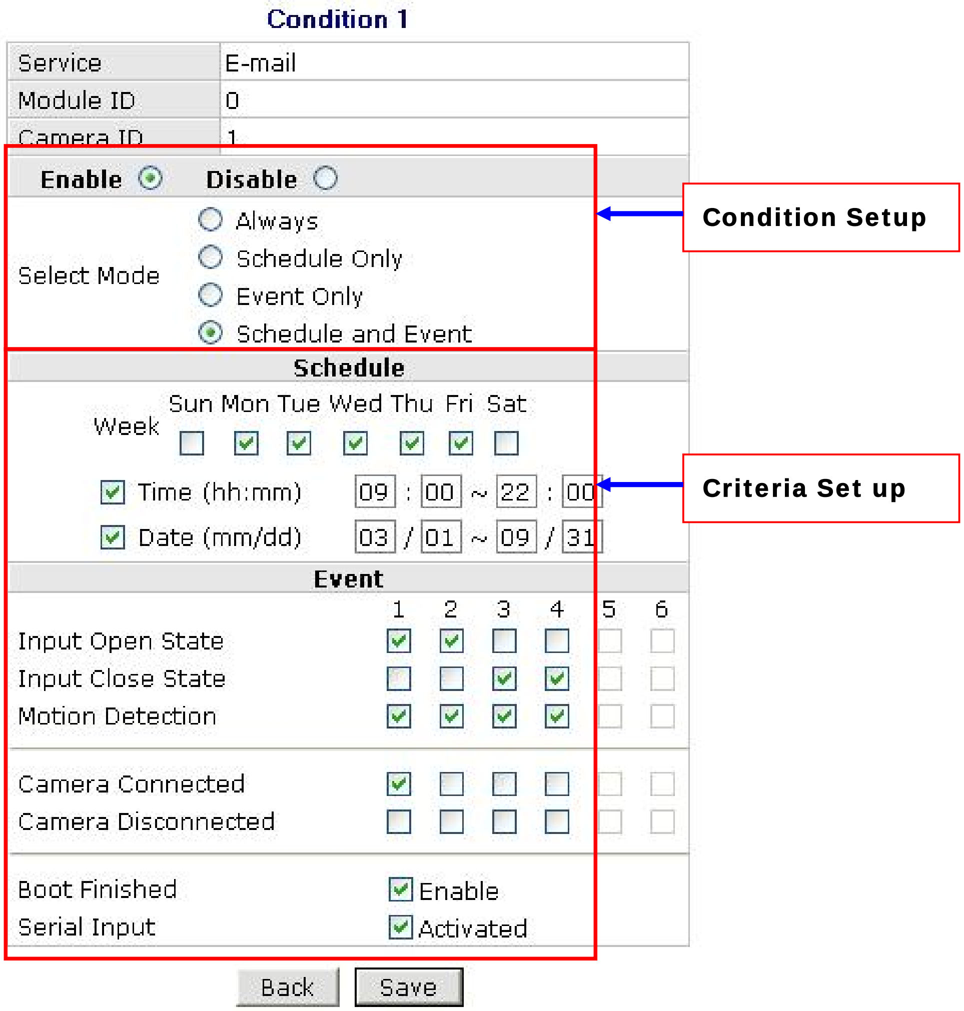
3) Click "**Buffer Calculator**" button to run the calculator

4) Pre configure pre/post alarm buffer for each service. This previous window can be open till you manually disclose the Window. Thus, you can refer to this table when you configure e-mail, ftp or Alarm buffering service configuration.

2 Service Condition

Sophisticated advanced services can be done by lots of serviced conditions provides by the system. To correctly set up the system use must has good understanding about the service condition as well.

e-mail, FTP, Sensor notification and Alarm output device control function requires service condition set up to activate the function. Note that the basic logic for the service condition set up is same for all of other options.



Condition 1

Service	E-mail
Module ID	0
Camera ID	1

Enable ● **Disable** ○

Select Mode
- ○ Always
- ○ Schedule Only
- ○ Event Only
- ● Schedule and Event

Schedule

Week	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	☐	☑	☑	☑	☑	☑	☐

☑ Time (hh:mm) 09 : 00 ~ 22 : 00

☑ Date (mm/dd) 03 / 01 ~ 09 / 31

Event

	1	2	3	4	5	6
Input Open State	☑	☑	☐	☐	☐	☐
Input Close State	☐	☐	☑	☑	☐	☐
Motion Detection	☑	☑	☑	☑	☐	☐
Camera Connected	☑	☐	☐	☐	☐	☐
Camera Disconnected	☐	☐	☐	☐	☐	☐

Boot Finished ☑ Enable

Serial Input ☑ Activated

Condition Setup

Criteria Set up

2.1 Condition Setup

This is to define basic condition to activate any option selected. Select right condition from the option provided.

Always :

To active any selected option regardless condition. If you select this condition Schedule and Event condition window become inactive.

Schedule Only :

To active any selected option by scheduling. If you select this criteria, Event condition setup window become inactive

Event Only :

To activate any selected option by Event only. Sensor status change is recognized as Event.

Schedule and Event :

To active any selected action when Event is triggered for the specified time period only. If Event is incurred out of Scheduled period, no action will be done.

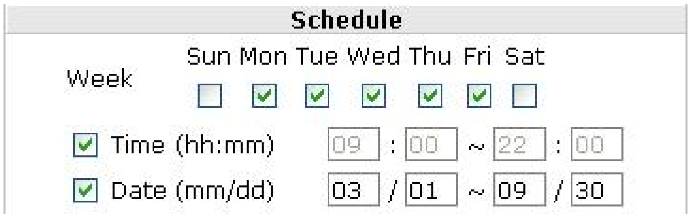
2.2 Criteria Setup

Once condition is selected, you need to set up event criteria following which any selected service will be executed.

Criteria consist of Schedule and Event which included Sensor input trigger, Boot finish and Serial input data trigger.

2.2.1 Schedule

You can select the day from the week. If you uncheck Sun and Sat, Sun and Sat will be excluded from the condition. If you enable Time only and disable Day of week and Date, any action taken place during specific time of the day, will be effective regardless day of week and Date of the year.



Schedule

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Week	☐	☑	☑	☑	☑	☑	☐

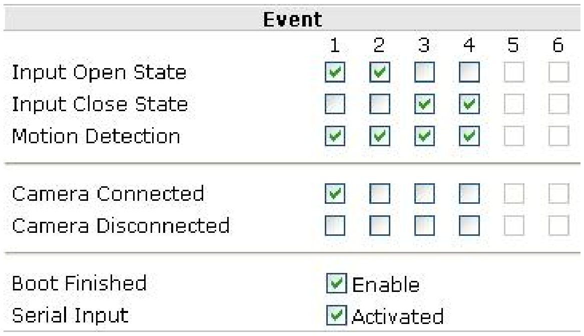
☑ Time (hh:mm) 09 : 00 ~ 22 : 00

☑ Date (mm/dd) 03 / 01 ~ 09 / 30

Above setting tells you that any action (e-mail, FTP or other services) will be done if any event is happened from 9AM to 10PM from Monday to Friday from March to September of the year.

2.2.2 Event

Alarm senor, Server reboot and Serial device activation or combined activation can be recognized as an event .



Event	1	2	3	4	5	6
Input Open State	☑	☑	☐	☐	☐	☐
Input Close State	☐	☐	☑	☑	☐	☐
Motion Detection	☑	☑	☑	☑	☐	☐
Camera Connected	☑	☐	☐	☐	☐	☐
Camera Disconnected	☐	☐	☐	☐	☐	☐
Boot Finished	☑ Enable					
Serial Input	☑ Activated					

Event number can be mapped as a Sensor port and camera number.

DI Open State :

This means that sensor is triggered and become open status from Normal close status. Select this when you use NC(Normal Close) type sensor.

DI Close State :

This means that sensor is triggered and become close status from Normal open. Select this when you use NO (Normal Open) type sensor.

Motion Detection :

By selecting this option, motion detection based event can be configured.

Camera Connected and Disconnected:

Camera status change by lost of camera signal can be recognized as an event

Boot Finished :

Boot finish means Server reboot. Thus, when the server is rebooted, it can be recognized as an event.

Serial input :

FlexWATCH^{TM} server can carry serial data along with video. When serial data from external serial device is activated, this can be recognized as a event.

Sensor state means when the sensor status is Open or closed. **If you use NC(Normal Close) type sensor and activate any action when sensor is open, you need to select [Open State] and vice versa when you use NO (Normal Open) type of sensor**.

Please check out sensor type connected to FlexWATCH^{TM} server

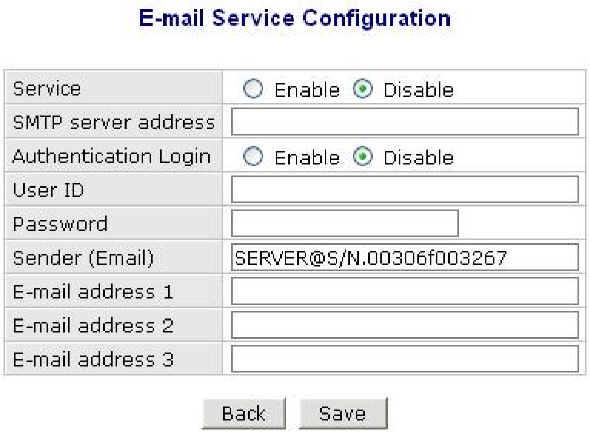
3 e-mail configuration

Schedule, event or schedule and event driven e-mail sending is supported by the server so that when there is any pre-configured event is happened, e-mail notice will be sent to any e-mail account.

3.1 e-mail function configuration

Up to 10 pre/post alarm image can be appended and sent through one e-mail when the event happens. By configuring pre/post alarm for e-mail, you can decide the number of image to be sent by an e-mail.

1) Go to Advance service mode in the Service configuration section
2) Go to Buffering service mode and set up pre/post alarm image for e-mail.
3) Select e-mail option from menu
4) Set up e-mail account in the e-mail configuration. This setting will be applied for all cameras.


E-mail Service Configuration

Service	○ Enable ● Disable
SMTP server address	
Authentication Login	○ Enable ● Disable
User ID	
Password	
Sender (Email)	SERVER@S/N.00306f003267
E-mail address 1	
E-mail address 2	
E-mail address 3	

SMTP Service address :

This is sending mail server address of ISP from which you get Internet access service. To get this info, consult with your Internet service provider or check the e-mail setting in your e-mail program such as outlook or Eudora.

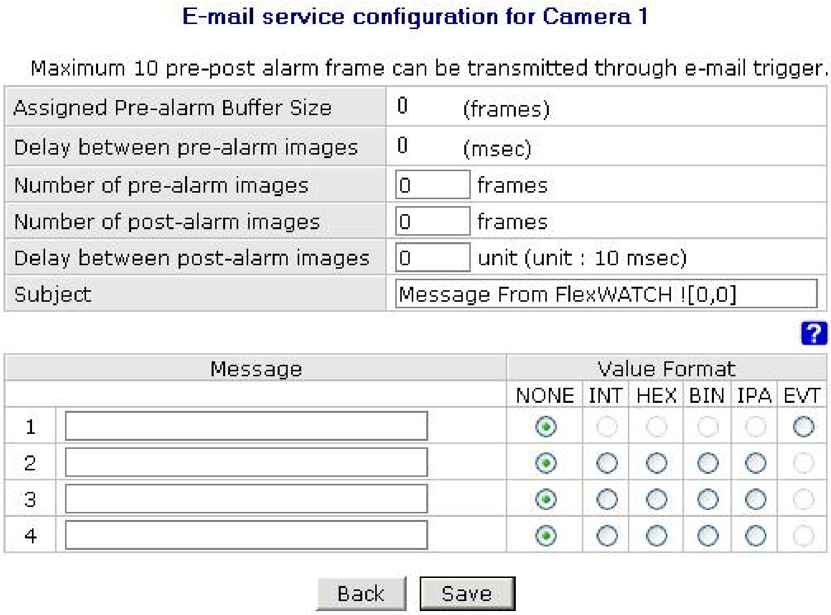
Authentication Login:

Now these days most of ISP is try to authenticate sender e-mail address due to security and spam mail issue. If sender authentication is enabled by your ISP, you need to get your login ID and Password from your e-mail service provider.

Sender (E-MAIL): put the sender e-mail. If you use system default sender e-mail address, it will not work.

E-mail address 1~ 3: put recipient e-mail address. Up to 3 different e-mail account can be supported.

5) Select channel to configure e-mail for each camera after setting up e-mail account



E-mail service configuration for Camera 1

Maximum 10 pre-post alarm frame can be transmitted through e-mail trigger.

Assigned Pre-alarm Buffer Size	0 (frames)
Delay between pre-alarm images	0 (msec)
Number of pre-alarm images	0 frames
Number of post-alarm images	0 frames
Delay between post-alarm images	0 unit (unit : 10 msec)
Subject	Message From FlexWATCH ![0,0]

	Message	Value Format					
		NONE	INT	HEX	BIN	IPA	EVT
1		●	○	○	○	○	○
2		●	○	○	○	○	○
3		●	○	○	○	○	○
4		●	○	○	○	○	○

Number of Pre alarm images :

Number of pre-alarm image should be less than Assigned Pre-alarm buffer size and maximum number of pre-alarm can not exceed 10 frames

Number of post-alarm images:

Less than 10 frames can be assigned as post-alarm images. Post alarm has nothing to do with Pre alarm buffer size.

Note that the sum of pre and post alarm can not exceed 10 frames.

Value Format :

Value strings can be sent together with e-mails. Please click "?" mark in the admin page to get more information.

3.2 e-Mail condition set up

Up to 3 different e-mail conditions can be set up for each camera. Schedule, event or schedule & event driven e-mail condition can be set up to send e-mail.

1) Run the e-mail condition set up window from the e-mail service configuration for each channel.
2) Check "**Enabl**e" field
3) Select mode for e-mail trigger and set up condition.

4 FTP Configuration

Schedule, event or schedule and event driven FTP functions supported by FlexWATCH^{TM} server so that when there is any pre-configured event is happened, image will be sent and stored in the FTP server.

Buffered FTP and Periodic FTP function is supported by FlexWATCH^{TM}. Buffered FTP means that ftp will be done when any event is occurred, i.e. change of status is generated and only pre/post alarm buffered image can be sent to FTP server.
Periodic FTP means that image will continuously be sent to FTP server when there is any event. No pre/post alarm image will be sent to FTP server.

4.1 Directory option

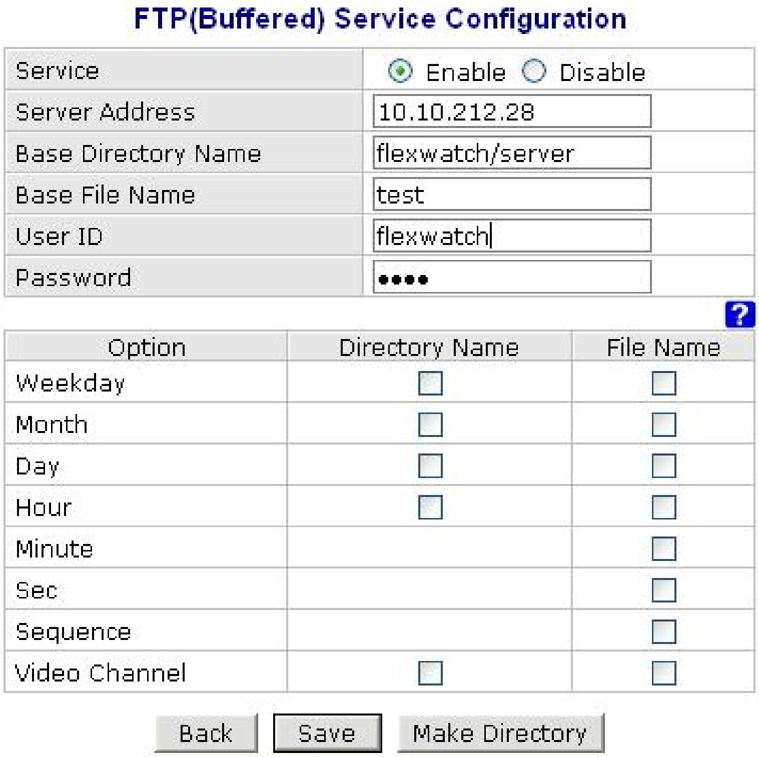
FlexWATCH^{TM} server provides powerful directory options so that user can easily create multiple ftp directory and send image into classified file directory as well.
Depends on the service type, Buffering and None buffering Service, its directory option is

slightly different.

4.1.1 Directory option for Buffered FTP

Buffered FTP means that only pre/post alarm buffered image will be sent to FTP server when the ftp is triggered by the event.

FTP function of FlexWATCH^{TM} server has two different level of directory and file name option and following are details.



FTP(Buffered) Service Configuration

Service	● Enable ○ Disable
Server Address	10.10.212.28
Base Directory Name	flexwatch/server
Base File Name	test
User ID	flexwatch
Password	●●●●

Option	Directory Name	File Name
Weekday	☐	☐
Month	☐	☐
Day	☐	☐
Hour	☐	☐
Minute		☐
Sec		☐
Sequence		☐
Video Channel	☐	☐

Base Directory Name :

Base directory is a path where ftped image will be saved in the FTP server. Directory name can be made under "ROOT" or "Home" directory of FTP server.

If you select directory name in the option filed above, sub-directory will be created under the Base Directory. If you do not select Directory option and select File Name option filed only, file name will be created with combination of Base File Name in the Base Directory.

Base File name :

User defined prefix of file name of each image. File name of FTP images will automatically be concatenated after prefix(Base File name).

Directory name :

Multiple directories can be created in the Base directory so that ftp image can be stored in a classified directory.

Once you select Directory name filed and click "**Make Directory**" button, multiple sub-directories will automatically be created in the Base directory according to selected option. Only one directory option among the multiple options can be selected.

Example) If you select "**Weekday**" option in the filed and Based file name is **flexwatch/server,** following sub-directory will automatically be created.

:/flexwatch/server/

Sun
Mon
Tue
Wed
Thu
Fri
Sat

File name :

File name will automatically be created with the prefix (the Base file name).

Multiple file name option field can be selected at the same time. In this case, each Field is concatenated sequentially But total length of file name is 32 characters including based directory name.

4.1.2 Directory option for Periodic FTP (Duration Service)

Configuration of Directory option for periodic is same as those of buffered service.

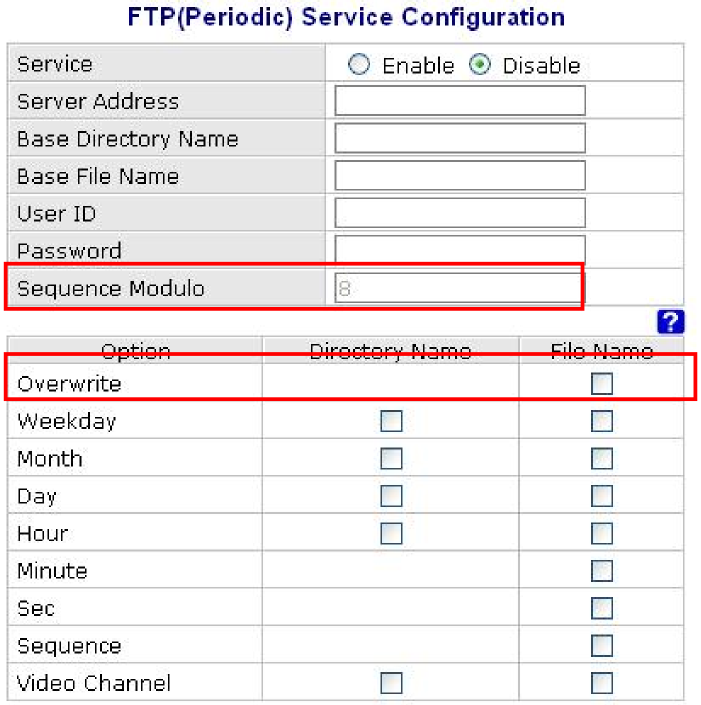
The only difference is that there are **Sequence Modulo** and **Overwrite option** in the option filed.

Sequence Modulo :

This is used when some number of ftp images should be stored and refreshed as new ftp images are stored in the ftp server. By setting up Modulo number for sequence, you can limit number of image to be stored and refreshed. If you set it as 8, 8images will be stored in the FTP directory and FIFO(first come, first out) based image will be saved in the FTP server.

Overwrite:

This is to refresh old image with new image in the ftp server. This is normally used when the ftped image should be refreshed every time.



FTP(Periodic) Service Configuration

Service	○ Enable ● Disable
Server Address	
Base Directory Name	
Base File Name	
User ID	
Password	
Sequence Modulo	8

Option	Directory Name	File Name
Overwrite		☐
Weekday	☐	☐
Month	☐	☐
Day	☐	☐
Hour	☐	☐
Minute		☐
Sec		☐
Sequence		☐
Video Channel	☐	☐

4.2 FTP service configuration

If you get good understanding of Pre/post alarm buffering and FTP directory option, now you can easily configure FTP function of the system.

Please make sure that you have your own FTP server and create Based directory in the FTP server.

4.2.1 Buffered FTP service

Buffered FTP means that rising or falling edge based ftp will be done when there is any event and only pre/post alarm buffered image can be sent to FTP server.

1) Go to **Advance Service** menu in the service configuration mode and select **Buffering Service** option

2) Set up Pre alarm buffering configuration for FTP service

3) Set up FTP directory and file name option

4) Select the camera and set up FTP condition for each camera. Up to 3 different ftp condition can be set up for each camera.

4.2.2 Periodic FTP service

Periodic FTP means that image will continuously be sent to FTP server when there is any event. No pre/post alarm image will be sent to FTP server.

1) Go to **Advance Service** menu in the service configuration mode and select **None Buffering Service** option

2) Set up FTP directory and file name option

3) Select the camera and set up FTP condition for each camera.

Example 1)

Let's suppose that a Camera takes a image every 15min and sends it to FTP server continuously. And the images are being accumulatively stored under the directory, namely 'FlexWATCH', in the FTP server for one year.

(Before starting this configuration, you must create a cetain directory name in the FTP server. The directory name 'FlexWATCH' is only an example.)

1) Go to '**Advanced Services** –> **Non-buffering Service** -> **FTP(Periodic)** -> **Camera1** -> **Condition1**' on the Admin menu.

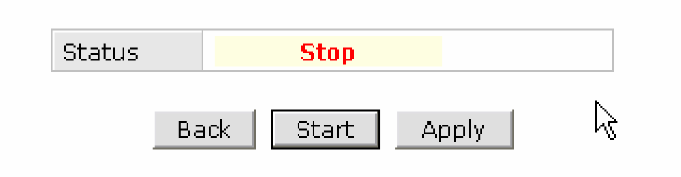
- Select 'Enable' and 'Always', then click 'Save'.

2) Go to '**Camera 1**' menu.

- Input **90000** units at '**Delay between Images'** and click 'Save'.

3) Go to '**FTP (Periodic)**' menu. Please set up as below, then click 'Save'.

4) Go to 'Advanced Services' menu.



- Click '**Apply**' button to apply the new service configuration as above.
- Close the window of 'Admin menu'. When 'Save configuration' window pop-up, click 'Save Configuration'.

Application idea

If server is connected to dynamic IP or Private network and you want to continuously send image to FTP server, please use Overwrite function in the Periodic FTP service.

5 Alarm Buffering Service

Pre/Post alarm image can be stored in the system memory so that user can remotely connect the server and playback stored image at any time.

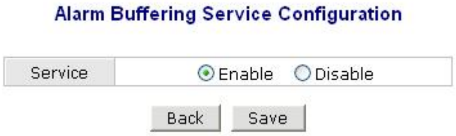
5.1 Alarm Buffering Service Configuration

1) Go to **Advance Service** menu in the service configuration mode and set up system memory assignment for Alarm Buffer service.

2) Select "**Buffering Service"** option and check whether **Pre Alarm buffer size** is already assigned. Otherwise, assign pre alarm butter size

3) Select "**Alarm Buffer Service**" from the listed option

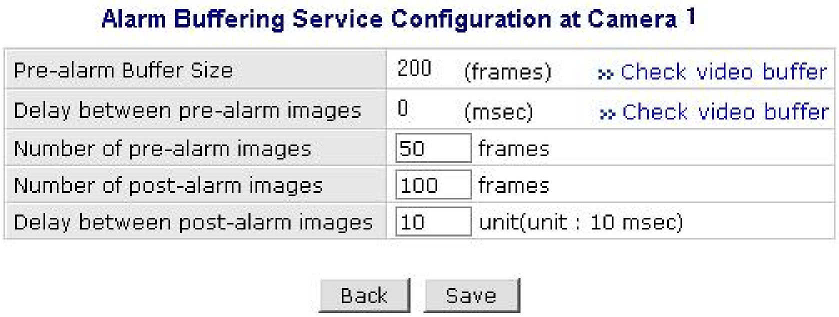
4) **Enable** the Alarm buffering service.



Alarm Buffering Service Configuration

Service	● Enable ○ Disable

5) Select the camera and assign Pre/post alarm image frames.



Alarm Buffering Service Configuration at Camera 1

Pre-alarm Buffer Size	200 (frames)	» Check video buffer
Delay between pre-alarm images	0 (msec)	» Check video buffer
Number of pre-alarm images	50 frames	
Number of post-alarm images	100 frames	
Delay between post-alarm images	10 unit(unit : 10 msec)	

6) Click "Save" button to memorize your new setting in the system.

7) Click the Condition menu and set up alarm buffering service condition.

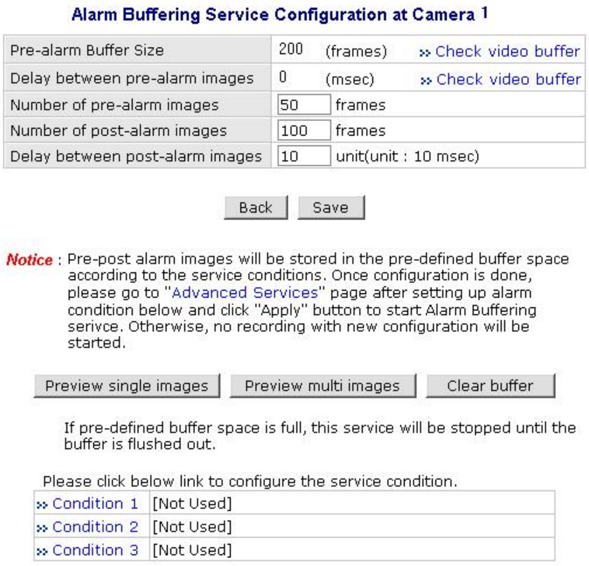
8) Click "**Advance Service**" menu in the Admin window and click "**Stop and Apply**" button to start record alarm triggered image in the system memory.

☞ ***Note that "Stop & Apply" button in the Advance Service window must be refreshed by clicking the button to start recording of any video in the memory. Otherwise no pre/post alarm image can be stored.***

5.2 Playback of Pre/post alarm Image

Once Alarm buffering service configuration is correctly done and pre/post alarm image is stored, any stored Pre/post alarm image can remotely playback through admin window.

1) Click Alarm Buffering Service menu from the Advance Service configuration menu



Alarm Buffering Service Configuration at Camera 1

Pre-alarm Buffer Size	200 (frames)	Check video buffer
Delay between pre-alarm images	0 (msec)	Check video buffer
Number of pre-alarm images	50 frames	
Number of post-alarm images	100 frames	
Delay between post-alarm images	10 unit(unit : 10 msec)	

Notice : Pre-post alarm images will be stored in the pre-defined buffer space according to the service conditions. Once configuration is done, please go to "Advanced Services" page after setting up alarm condition below and click "Apply" button to start Alarm Buffering serivce. Otherwise, no recording with new configuration will be started.

If pre-defined buffer space is full, this service will be stopped until the buffer is flushed out.

Please click below link to configure the service condition.

Condition 1	[Not Used]
Condition 2	[Not Used]
Condition 3	[Not Used]

Preview Single Images:

This is to view image one by one.

Preview Multi images:

You can view panoramic images of all the saved images at a glance.

2) Click Preview Single Imager or Preview Multi images option to playback.

3) Click "**Clear Buffer**" to delete all archived images

☞ ***Note***

Note that if you cleared the buffered image and want to save new images in the memory, you need to go to Initial page of Advance Service configuration menu and click "**Stop & Apply**" button to refresh the buffer images.

Application Idea

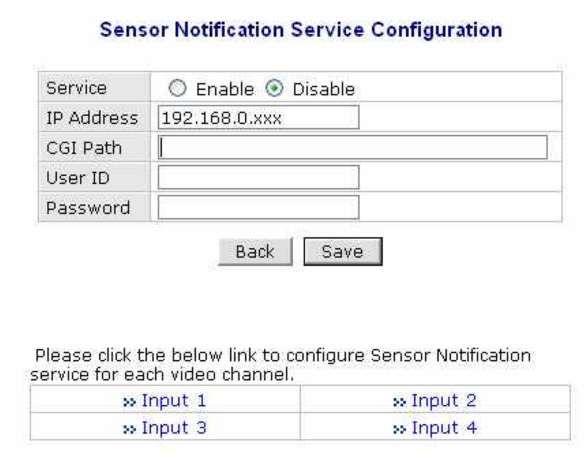
If you would like to download buffered images and save them in Client PC, please contact your vendor or manufacturer to get in-depth technical documentation.

6 Sensor Notification service

Sensor Notification service is to send alarm trigger information to third party application program through CGI Patch. This option is to invoke third party application program upon receipt of sensor information from FlexWATCH™ server.

1) Go to Advance service configuration of Service configuration mode

2) Click None buffering service mode and go to sensor notification service



Sensor Notification Service Configuration

Service	○ Enable ● Disable
IP Address	192.168.0.xxx
CGI Path	
User ID	
Password	

Please click the below link to configure Sensor Notification service for each video channel.

» Input 1	» Input 2
» Input 3	» Input 4

IP Address : IP address of target device to which sensor notification will be sent

CGI Path : Common Gateway Interface to the Application program

User ID / Password : Authentication ID and Password of the application program.

3) Type in CGI Path and User ID & Password to third party application program.

4) Select sensor input number

5) Type CGI Name (User definable) and set up condition to trigger Sensor notification function.

Utilities

Utilities is to manage and control system properly. **Save Configuration, Flash Update, System Reboot and system upgrade options** are provided.

1 Save Configuration

This is to save all new configuration and settings in the system memory. Once new configuration is saved by "**Save Configuration**" menu, new configuration will permanently saved in the system memory **only after system Reboot or system power off**

2 Reboot

Reboot means restart system. It is needed to reinitialize and restart system after changing some configurations that has influence on the system.

Thus, it is highly recommended to reboot the system after executing "Save Configuration" menu.

Most of case system reboot comes last only after all the new configuration is done. But some of system menu require system reboot in the middle of system configuration so that new setting can properly applied in the system.

Followings are list of option which require System reboot.

- **Network Configuration**
- **Date & Time configuration with Time Zone change**
- **Serial Port configuration**
- **Memory assignment for Advance Service**
- **Factory Default**

☞ ***Note***

System reboot requires about 1Minutes of lead time. Thus, if you execute Reboot option, please wait at least 1minutes to do other settings.

3 Factory Default

Factory Default is to reset all the configuration of the system as the initial status except Network Configuration. This utility is recommended to use only when you lost all of your logics for system configuration, since executing this option Except Network configuration will lose all of your setting.

4 System Update

System update can remotely be done through web page of the system or ftp option with telnet and Hyper Terminal mode. In this user manual only web based system update method is described and ftp based system update method can separately provided.

4.1 Description of files system

FlexWATCH™ Server has 4 different files to get the system work. In some case, you may need to upgrade whole files or other case you need to upgrade some specific file only. Following is brief explanation about the file system for FlexWATCH™ server.

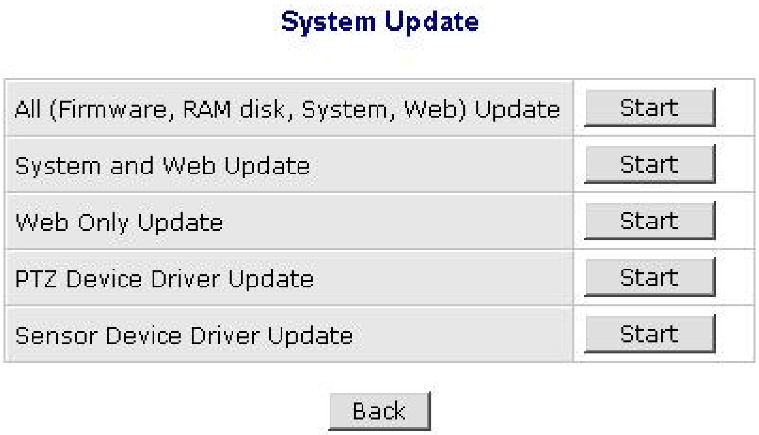
Files*	Size (unit : KB) **	Description
e_ker_xx	629	Kernel file – Same as Os in the window.
e_rfs_xx.gz	1.547	Root file system
e_sys_xx.tar.gz	975	System file – Application software in the window
e_web_xx.tar.gz	435	Web file – Web server of FlexWTCH™ server

* *Note depending on the hardware initial of each file can be different.*

** You can download the latest version from "Downloads" menu on www.flexwatch.com, www.seyeon.co.kr.

** file size will be different in each version

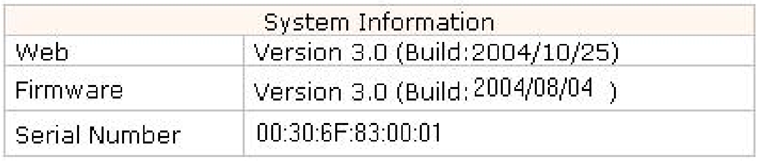
In addition to above 4files, PTZ device driver and Sensor Device Driver module can separately uploaded into the system through web browser.



System Update

All (Firmware, RAM disk, System, Web) Update	Start
System and Web Update	Start
Web Only Update	Start
PTZ Device Driver Update	Start
Sensor Device Driver Update	Start

Back



System Information	
Web	Version 3.0 (Build:2004/10/25)
Firmware	Version 3.0 (Build: 2004/08/04)
Serial Number	00:30:6F:83:00:01

All (kernel, RAM disk, System, Web) Update:

To completely update all the system for Kernel, RAM Disk, System and Web all together except PTZ Device Driver or Sensor Device Driver. This option is recommended if there is special notice by manufacturer. Generally complete system update comes only when there is big change for all of the system software.

System and Web Update:

To update system and web related software together. This update can be common to update the system.

Web Only Update:

To update only Web page of the server. This is useful to uploaded customized web page only to save update times.

PTZ Device Driver :

PTZ Device Driver is already built-in the system. But if there is a new PTZ Device driver supported by the system, it can separately uploaded into the system without other software change.

Sensor Device Driver :

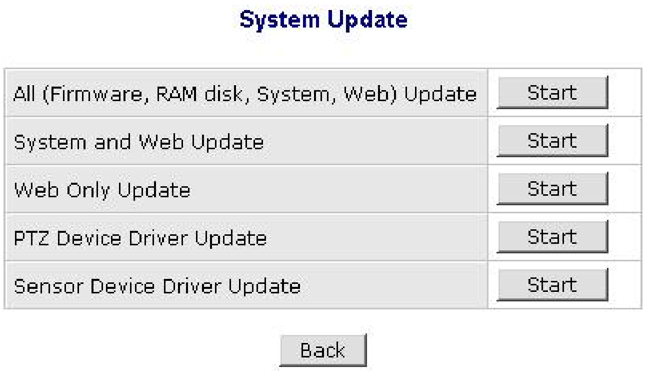
Serial input device driver can separately be uploaded into the system so that independent Serial input device can work with FlexWATCH^{TM} Server.

4.2 Update Procedure

Step by step procedure is provided by the system which means, each file will separately uploaded one by one.

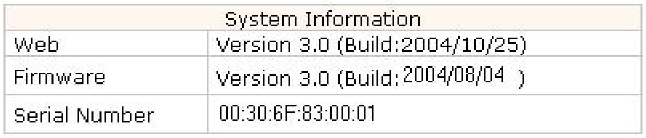
Please make sure that all the system files to be updated reside in your PC before starting update.

1) Go to **Utilities** column and select "**System update**" option
2) Select option provided in the system update window and click "**Start**" button.



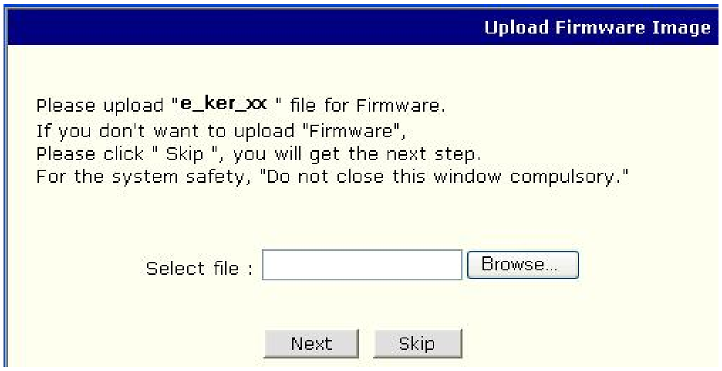
System Update

All (Firmware, RAM disk, System, Web) Update	Start
System and Web Update	Start
Web Only Update	Start
PTZ Device Driver Update	Start
Sensor Device Driver Update	Start



System Information	
Web	Version 3.0 (Build:2004/10/25)
Firmware	Version 3.0 (Build: 2004/08/04)
Serial Number	00:30:6F:83:00:01

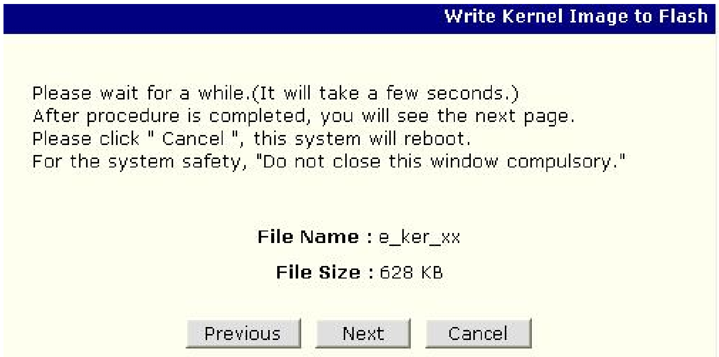
3) Browse your pc and select the right file to update following the update guide. If you want to skip specific update, click "**Skip**" button.


Upload Firmware Image

Please upload "e_ker_xx " file for Firmware.
If you don't want to upload "Firmware",
Please click " Skip ", you will get the next step.
For the system safety, "Do not close this window compulsory."

Select file :
Browse...
Next
Skip

4) Once update is successfully done following result will come up.


Write Kernel Image to Flash

Please wait for a while.(It will take a few seconds.)
After procedure is completed, you will see the next page.
Please click " Cancel ", this system will reboot.
For the system safety, "Do not close this window compulsory."

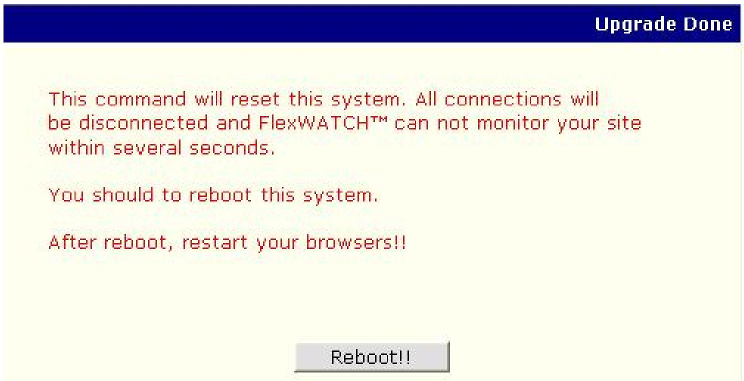
File Name : e_ker_xx

File Size : 628 KB

Previous
Next
Cancel

5) If you want to update RAM Disk, System and web page, please click "Next" button follow the web guide to update more files.

6) If all of file update is finished "System Reboot" window will come and do system reboot to apply new update.


Upgrade Done

This command will reset this system. All connections will be disconnected and FlexWATCH™ can not monitor your site within several seconds.

You should to reboot this system.

After reboot, restart your browsers!!

Reboot!!

Warranty

Product	Network Video Server		
Model	FlexWATCH^{TM} 3440		
S/N			
A/S	Seyeon Tech Ltd.	Warranty	1 year Limited
	+82-2-3017-0866	www.flexwatch.com	

Seyeon Tech Co., Ltd.

TEL : +82-2-3017-0855
FAX : +82-2-3017-0843
http://www.seyeon.co.kr
http://www.flexwatch.com

A/S Center:
Tel : +82-2-3017-0855
Fax: +82-2-3017-0843